IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

Amanda Christenson, Taisha Dixon, Tracy Anne Phillips, Paul Avery, Jacqueline Jackson, Robin Dugan, Tawfik Mammad, Zoe Madonna, Kali Warren, Bethany Conley, Brittany Meadows, Olga Diatlova, Lashanden Darby, Edith Antonio, Amanda Rape, Deana Leffers, M.O., Joshua Lowe, Rene Sims, Hailey Kleinheksel, Michelle Carter, Marissa Hatfield, Cedric Bonier, Jan Merrill, Richard Seibert, Michael Paul, DeBorah Evans, Lisa Brooks, David Powers, Roxanne Allen, Patricia Baggett, Kenya Jones, Edwin Hoag, Richard Schwalbe, Delmar Kentner, Dawn Duncan, Rosa Rubera, Matthew Loforese, Carol Slack, Rachael Schiller, Tristano Korlou, Patricia Donadio, James Morgan, Kaela Poitra, Autumn Abramczyk, Anna Griffith, Preslee Thorne, Robin Lanier, Ashley Harbon, Kim Kaehler, Sally Kirkpatrick, Tess Bussick, Lori Tynch, Polly Rush, Anna Lovell, Christina Estep, Alfred Williams, Sr., Angela Johnson, Trudy Agres, Leigh Thompson (Tom) Hanes, J'Andre Ivory, Harry Knopp, Mark Wetzel, Luke Anderson, and Lauren Fossen, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

UnitedHealth Group Incorporated, Optum, Inc., OptumInsight, Inc., and Change Healthcare Inc.,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

INTRODUCTION

Plaintiffs[1] individually and on behalf of all other similarly situated, upon personal knowledge of facts pertaining to themselves against Defendants UnitedHealth Group Incorporated ("UHG"), Optum, Inc. ("Optum"), OptumInsight, Inc. ("Optum Insight") and Change Healthcare Inc. ("Change Healthcare") (collectively, "Defendants"), and in support thereof allege as follows:

NATURE OF THE ACTION

1. Plaintiffs are among the tens of millions of individuals in the United States who had their sensitive, personally identifiable information ("PII") and protected health information ("PHI" and together with PII, "Personal Information") stolen from a database operated by Defendants. Starting on February 21, 2024, hackers successfully breached Defendants' database, accessed decades-worth of personal and medical data, and exfiltrated the Personal Information of over 120 million patients (the "Data Breach"). The result was the largest ever healthcare data breach in the United States.[2]

2. Defendants, and, in particular, Change Healthcare, gathered and collected this vast volume of Personal Information through their business operations. As a clearinghouse for over 50% of all medical claims in the United States, Change Healthcare obtained access to the data involved in billions of medical transactions, allowing it to

[1] "Plaintiffs" refer collectively to all individuals named as Plaintiffs in this Complaint.
[2] Steve Adler, *Nebraska Sues Change Healthcare Over February Ransomware Attack*, The HIPAA Journal (Dec. 17, 2024), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ (last visited Dec. 15, 2024).

aggregate substantial amounts of medical records, histories, and information on millions of individuals.

3. Change Healthcare, and later the other Defendants, used the collected Personal Information for their own benefit. Specifically, Defendants commoditized the sheer volume of Personal Information by, among other things, using it to run analytics and selling the analyses to insurers, including one of Defendants' sister companies, UnitedHealthcare, Inc.

4. In 2022, UHG finalized a deal to acquire Change Healthcare and merge it into one of its subsidiaries, Optum Insight. The goal of the acquisition was clear: to allow UHG, Optum and Optum Insight access to the Personal Information of one in three Americans.[3] With this vast amount of highly sensitive Personal Information, Defendants sought to retain and use it for one express goal: profit.

5. While Defendants held the Personal Information of over 100 million Americans, they failed to use even basic data security measures necessary to protect it.

6. On or around February 12, 2024, a ransomware group known as ALPHV, and its affiliates, compromised Change Healthcare (which had since merged with Optum Insight) and gained access to its systems. Although many details of the Data Breach have

[3] *United Health CEO estimates One-Third of Americans Could be Impacted by Change Healthcare Cyberattack*, (May 20, 2024), http https://www.cnbc.com/2024/05/01/unitedhealth-ceo-one-third-of-americans-could-be-impacted-by-change-healthcare-cyberattack.html.

not been publicly released, the nature of the breach illustrates Defendants' severe security deficiencies.

7. Specifically, ALPHV was able to gain access to large quantities of Personal Information by compromising a single employee's remote access credentials. The hacking group used the "compromised [password] credentials to remotely access a Change Healthcare Citrix [Remote PC Access] portal, an application used to enable remote access to laptops."[4] The compromised credentials were from a relatively low-level employee and likely obtained through common, well-known tactics like phishing.[5]

8. Had Defendants employed basic, long-established, and recommended security tools, the Data Breach should have been easily thwarted. However, Defendants' "[Citrix Remote PC Access] portal did not have multi-factor authentication," among other failures, meaning ALPHV had virtually no roadblocks in gaining access to the large quantities of Personal Information Defendants stored.[6]

---

[4] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

[5] *Nebraska AG files lawsuit against Change Healthcare after 'historic' data breach*, (Dec. 16, 2024), https://www.1011now.com/2024/12/16/attorney-general-mike-hilgers-files-lawsuit-against-change-healthcare-critical-failures-protect-consumer-data-prevent-against-harm-widespread-cyberattack/.

[6] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

9. Once in Change Healthcare's networks, ALPHV "moved laterally within the systems" and successfully "exfiltrated data"—that is, removed the data—from Defendants' server.[7] Despite its sensitivity, Defendants did not store the data in an encrypted format and do not appear to have properly segregated the data from other parts of the network. Both indicate massive security failures.

10. Nine days later, on February 21, 2024, the ALPHV hackers were still undetected by Defendants' data security tools, demonstrating a lack of adequate logging and monitoring of the important and sensitive areas of Defendants' systems. The hackers successfully deployed ransomware on Defendants' networks, "encrypting Change Healthcare's systems so" they could not be accessed without ALPHV's cooperation.[8]

11. Following the ransomware deployment, Defendants were completely unable to recover their systems. As a result, Defendants paid $22 million in Bitcoin to ALPHV to regain access.[9] Defendants' decision to pay a ransom runs counter to law enforcement's recommendations, as nothing requires the hackers to keep their word that they will destroy the data after payment—and they often do not.

12. The ransom payment did nothing to benefit the Plaintiffs, the Class or the millions of others impacted by the Data Breach. By the time Defendants paid the ransom, the hackers had already walked away with the Personal Information of one-third of the

---

[7] *Id.*
[8] *Id.*
[9] Ashley Capoot, *UnitedHealth CEO tells lawmakers the company paid hackers a $22 million ransom*, CNBC (May 1, 2024), https://www.cnbc.com/2024/05/01/unitedhealth-ceo-says-company-paid-hackers-22-million-ransom.html.

United States, including Plaintiffs' and the Class's data. Indeed, another ransomware group, RansomHub, confirmed that it possessed four terabytes of stolen data from the Data Breach and has posted screenshots of the data on its dark web ransomware site. The hackers continue to attempt to extort Defendants out of additional ransom payments.[10] Now that Defendants have recovered their own copies of the data allowing them to continue to monetize it, however, they appear less eager to pay any further ransom. As a result, Plaintiffs' and the Class's data will likely wind up on the dark web to the extent it is not there already.

13. Both before and after the Data Breach, Defendants repeatedly put their interests above those of the impacted patients. However, Defendants owed duties to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Personal Information against unauthorized access and disclosure. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the Personal Information entrusted to them from unauthorized access and disclosure.

14. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred and Plaintiffs' and Class members' Personal Information was accessed by, and disclosed to, unauthorized third-party actors.

[10] Ionut Arghire, *Ransomware Group Starts Leaking Data Allegedly Stolen From Change Healthcare*, Security Week (Apr. 16, 2024), https://www.securityweek.com/ransomware-group-starts-leaking-data-allegedly-stolen-from-change-healthcare/.

15. Plaintiffs have experienced extensive harms as a result, including, among other things: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

16. This instant action seeks to hold Defendants accountable for their inadequate security and the resulting, largest ever healthcare Data Breach. Plaintiffs thus bring this Complaint on behalf of themselves, and all similarly situated individuals whose Personal Information was stolen as a result of the Data Breach. Plaintiffs, on behalf of themselves and all other Class members, bring the below common law tort claims and state statutory claims seeking declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

I. Plaintiffs

17. **Plaintiff Amanda Christenson is a citizen of Alabama** residing in Huntsville, Alabama. Plaintiff Christenson received a notice letter from Defendants dated August 5, 2024. On or about February 2024, she learned that there was a fraudulent attempt

to access her iCloud account. Since February 2024, Plaintiff Christenson has also received an increase in spam, including spam e-mails addressed to Robert Young, an individual who is unknown to her. The number of spam texts, calls, and e-mails she receives has increased from approximately 5-10 per day to approximately 20-30 per day. Since about April 2024, Plaintiff Christenson has been notified on multiple occasions that her sensitive personal information, including her Social Security Number and her email address, is on the dark web. Since about April 2024, she has experienced multiple attempts of unauthorized charges on various accounts, ranging from $4 to $250. For example, on or about July 2024, there were several fraudulent attempts to charge her CashApp account in the amounts of $0.08 - $10. On or about September 2024, there was a fraudulent attempted charge of $158 on her CashApp account. On or about January 2025, Plaintiff Christenson learned that an unauthorized individual applied for a loan on her behalf, which was reflected on, and negatively impacted, her credit report. When Plaintiff Christenson attempted to apply for a loan for herself, it was denied. Plaintiff Christenson estimates she spent about ten hours responding to the breach by researching the breach, contacting major credit bureaus to freeze her credit, monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, and contacting CashApp about the fraudulently attempted charges on her account. Plaintiff Christenson continues to review her accounts for fraud.

18. Prior to the Data Breach, Plaintiff Christenson had never experienced any type of fraud in her banking and credit card history. Plaintiff Christenson is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Christenson stores any and

all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

19. **Plaintiff Taisha Dixon is a citizen of Alaska** residing in Anchorage, Alaska. Plaintiff Dixon received a notice letter from Defendants dated September 3, 2024. Since February 2024, she experienced an increase in suspicious activity. This suspicious activity includes two instances of fraudulent charges on her Credit Union bank card totaling $43, five alerts from Credit Karma notifying her of potential changes to her credit history; and an increase in spam text messages and phone calls. Plaintiff Dixon estimates she spent about 30 hours responding to the Data Breach by researching the Data Breach, contacting her Credit Union about fraudulent activity and getting new bank cards issued, monitoring her accounts for suspicious activity and fielding spam/phishing calls. Plaintiff Dixon continues to review her accounts for fraud.

20. Plaintiff Dixon is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Dixon stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

21. **Plaintiff Tracy Anne Phillips is a citizen of Arizona** residing in Tucson, Arizona. Plaintiff Phillips received a notice letter from Defendants dated September 3, 2024. On or about February 2024, she learned that fraudulent charges were made on her credit card, and it happened again in July—despite having replaced her cards. Plaintiff Phillips estimates she spent about 80 hours responding to the Data Breach by contacting banks, credit card companies, or other vendors about fraudulent and suspicious activity. Plaintiff Phillips signed up for credit monitoring offered by Equifax and IDX Monitoring and continues to review her accounts for fraud.

22. Prior to the Data Breach, Plaintiff Phillips had never experienced any type of fraud in her banking and credit card history. Plaintiff Phillips is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Phillips stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

23. **Plaintiff Paul Avery is a citizen of Arkansas** residing in Jonesboro, Arkansas. Plaintiff Avery received a notice letter from Defendants dated September 3, 2024. Since February 2024, he has experienced an increase in spam emails and calls, including approximately five calls a week. Plaintiff Avery also learned that his Social Security number was on the dark web via notification from his Capital One credit

monitoring service. Plaintiff Avery not only changed the passwords on all his accounts, but he also increased their complexity.

24. Plaintiff Avery is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Avery stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

25. **Plaintiff Jacqueline Jackson is a citizen of California** residing in San Francisco, California. Plaintiff Jackson received a notice letter from Defendants dated September 3, 2024. On or about August 2024, she discovered that an Acorn account was opened and linked to her bank account, thereby allowing an unauthorized party to steal approximately $600. Plaintiff Jackson also received notice that her information was found on the dark web. Additionally, Plaintiff Jackson experienced an increase in spam calls and e-mails, including receiving 10-20 spam emails per day. For example, she received emails from an unknown person claiming they had her Personal Information and threatened to expose it if she did not pay $3,000. Plaintiff Jackson also experienced delays in medical care and the receipt of her prescription medication. Plaintiff Jackson estimates she spent about 50 hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity and investigating fraudulent/suspicious activity. Plaintiff Jackson continues to review her accounts for fraud.

26. Plaintiff Jackson is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Jackson stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

27. **Plaintiff Robin Dugan is a citizen of Colorado** residing in Peyton, Colorado. Plaintiff Dugan received a notice letter from Defendants dated September 3, 2024. In or about December 2024, she began receiving an influx of spam calls, often up to 25 each week. The spam callers often asked for her by name. Plaintiff Dugan estimates she spent about 3 to 4 hours responding to the Data Breach by researching the Data Breach, contacting her doctors to notify them about the Data Breach and putting a fraud alert on her credit. Since the Data Breach occurred, Plaintiff Dugan was notified by Experian that her information was found on the dark web. Plaintiff Dugan continues to review her accounts for fraud.

28. Prior to the Data Breach, Plaintiff Dugan had never experienced any type of fraud in her banking and credit card history. Plaintiff Dugan is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Dugan stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise

be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

29. **Plaintiff Tawfik Mammad is a citizen of Connecticut** residing in Avon, Connecticut. Plaintiff Mammad received a notice letter from Defendants dated July 29, 2024. On or about October 2024, he learned that a fraudulent store account was opened in his name at a Tommy Hilfiger store. Besides the fraudulent store account, Plaintiff Mammad has also received fraudulent invoices. Plaintiff Mammad estimates he spent significant time responding to the Data Breach by researching the Data Breach, contacting Defendants, monitoring his accounts for suspicious activity, investigating fraudulent or suspicious activity, filing a police report related to the fraudulent store account and contacting his banks and credit card companies about fraudulent or suspicious activity. Plaintiff Mammad signed up for the credit monitoring offered by Defendants and continues to review his accounts for fraud.

30. Prior to the Data Breach, Plaintiff Mammad had never experienced any type of fraud in his banking and credit card history. Plaintiff Mammad is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Mammad stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

31. **Plaintiff Zoe Madonna is a citizen of Delaware** residing in Wilmington, Delaware. Plaintiff Madonna received a notice letter from Defendants dated September 3, 2024. Since about September 2024, she received an increase in spam e-mails and texts. On or about September 2024, Plaintiff Madonna was notified that her passwords were leaked twelve times and she was notified that her Personal Information, including her e-mail address, was found on the dark web eight times. Plaintiff Madonna estimates she spent about five to seven hours responding to the Data Breach by monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, setting up an account to monitor password leaks, and changing passwords to accounts containing her Personal Information. Plaintiff Madonna signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

32. Plaintiff Madonna is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Madonna stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

33. **Plaintiff Kali Warren is a citizen of the District of Columbia** residing in Washington, District of Columbia. Plaintiff Warren received a notice letter from Defendants dated September 3, 2024. Since about June 2024, she was notified, via Experian, approximately sixty-two times that her Personal Information is on the dark web.

On or about October 2024, she experienced an increase in spam e-mails and texts, including multiple e-mails from a law group unknown to her stating that she owed them $6,000. She also received multiple threatening e-mails stating that she would face legal consequences if she did not pay certain amounts of money she did not actually owe. Plaintiff Warren estimates she spent approximately hundred hours responding to the Data Breach by contacting major credit bureaus to obtain her credit reports, assess whether they had been impacted by the fraud she experienced, and monitor accounts for suspicious activity. Plaintiff Warren signed up for the credit monitoring offered by Defendants, but it fails to report activity on her account. Kali Warren continues to review her accounts for fraud.

34. Plaintiff Warren is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Warren stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

35. **Plaintiff Bethany Conley is a citizen of Florida** residing in Panama City Beach, Florida. Plaintiff Conley received a notice letter from Defendant dated September 23, 2024. On or about December 2024, she received a text message to pay postage via USPS, and when she clicked the link to pay 30 cents, she was charged $2,500. Since February 2024, Plaintiff Conley has received an increase in daily spam calls, text messages, and emails. In addition, on September 26, 2024, she received notice from CreditWise that

her email and Social Security number was compromised and that her personal information was on the dark web. On October 6, 2024, Plaintiff Conley obtained a US Bank credit alert. As a result, Plaintiff Conley went without access to her card for approximately ten days. Plaintiff Conley estimates she spent about ten hours responding to the Data Breach by researching the Data Breach, contacting her card issuers and banks, monitoring her accounts for fraudulent activity, investigating suspicious charges, and changing passwords to all bank accounts. Plaintiff Conley continues to review her accounts for fraud.

36. Plaintiff Conley is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Conley stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

37. **Plaintiff Brittany Meadows is a citizen of Florida** residing in Jacksonville, Florida. Plaintiff Meadows received a notice letter from Defendants dated August 12, 2024. On or about February 26, 2024, Plaintiff Meadows tried to fill her prescription using her discount card through AbbVie's co-pay assistance program for her prescriptions at Capsule Pharmacy. Capsule Pharmacy was unable to process her discount card. On or about March 1, 2024, Plaintiff Meadows received a notice from Capsule Pharmacy informing her that the systems were down. On or about March 10, 2024, Plaintiff Meadows tried again to fill her prescription using her discount card with a different pharmacy, Publix Pharmacy,

however, Publix Pharmacy was also unable to process her discount card. Plaintiff Meadows had no alternative options but to pay $166 to receive her prescription that day, as opposed to paying $25. In addition, Plaintiff Meadows noticed an increase in phishing/unsolicited calls. Around February 2024, Plaintiff Meadows learned that her primary Gmail account was on the dark web. In or around October 2024, for approximately two weeks, Plaintiff Meadows received USPS notifications that she shipped out packages, however, she never did. Plaintiff Meadows believes some unknown actor had her address and was using it without her knowledge or consent. Plaintiff Meadows estimates she spent about 10 hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity, and talking to Capsule Pharmacy and Publix Pharmacy about the Data Breach. Plaintiff Meadows estimates she incurred $166 in out-of-pocket costs responding to the Data Breach by incurring prescription costs. Plaintiff Meadows continues to review her accounts for fraud.

38. Prior to the Data Breach, Plaintiff Meadows had never experienced any type of fraud in her banking and credit card history. Plaintiff Meadows is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Meadows stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

39. **Plaintiff Olga Diatlova is a citizen of Florida** residing in Miami, Florida. Plaintiff Diatlova received a notice letter from Defendants dated August 5, 2024. On or about June 2024, Plaintiff Diatlova learned that an unauthorized Bank of America checking account was opened in her name using her information. In addition, Plaintiff Diatlova noticed a substantial increase in suspicious phishing calls and emails. One email she received was threatening in nature, stating that an unknown individual would "expose her" if she did not pay them in Bitcoin. Around the same time, Plaintiff Diatlova learned that her information was found on the dark web. In or around October 2024, Plaintiff Diatlova experienced delays in healthcare and was no longer able to get insulin covered by her health insurance. Plaintiff Diatlova estimates she spent around four hours responding to the Data Breach by researching the Data Breach, contacting Bank of America, monitoring her accounts for suspicious activity, and investigating the fraudulent activity on her accounts. Plaintiff Diatlova continues to review her accounts for fraud.

40. Prior to the Data Breach, Plaintiff Diatlova had never experienced any type of fraud in her banking and credit card history. Plaintiff Diatlova is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Diatlova stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

41. **Plaintiff Lashanden Darby is a citizen of Georgia** residing in Hampton, Georgia. Plaintiff Darby received a notice letter from Defendants dated September 3, 2024. On or about August 2024, she learned that an unauthorized user attempted to open an account in her name. She also experienced an uptick in spam calls and e-mails, including receiving approximately four spam calls per day. Plaintiff Darby estimates she spent about twenty-five hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Darby continues to review her accounts for fraud.

42. Prior to the Data Breach, Plaintiff Darby had never experienced any type of fraud in her banking and credit card history. Plaintiff Darby is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Darby stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

43. **Plaintiff Edith Antonio is a citizen of Hawaii** residing in Pahoa, Hawaii. Plaintiff Antonio received a notice letter from Defendants dated September 3, 2024. On or about February 2024, she began receiving an increase in spam e-mails, phone calls and text messages. Specifically, she received approximately 3--4 spam emails per day, 2-3 spam phone calls per day, and 1-2 spam text messages per day. Plaintiff Antonio estimates she spent about 5 hours responding to the Data Breach by researching the Data Breach and

monitoring her accounts for fraudulent activity. Plaintiff Antonio continues to review her accounts for fraud.

44. Plaintiff Antonio is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Antonio stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

45. **Plaintiff Amanda Rape is a citizen of Idaho** residing in Orofino, Idaho. Plaintiff Rape received a notice letter from Defendants dated September 3, 2024. On or about July 31, 2024, she learned there was an attempted fraudulent charge in the amount of $889.60 on her Umpqua bank card for a flight from Argentina to Panama. As a result, she had to cancel her card and did not have access to it for about 24 hours. Since about February 2024, Plaintiff Rape has experienced an increase in spam and phishing calls, text messages, and e-mails. She receives several spam text messages per day. Plaintiff Rape has also been notified that her Personal Information was found on the dark web. Plaintiff Rape estimates she spent about 50 hours responding to the Data Breach by researching the Data Breach to gauge its severity, monitoring accounts for suspicious activity several times per day, and changing passwords for her PayPal account and bank accounts. Plaintiff Rape continues to review her accounts for fraud.

46. Prior to the Data Breach, Plaintiff Rape had never experienced any type of fraud in her banking and credit card history. Plaintiff Rape is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Rape stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

47. **Plaintiff Deana Leffers is a citizen of Illinois** residing in Quincy, Illinois. Plaintiff Leffers received a notice letter from Defendants dated September 23, 2024. On or about August 2024, she learned that her Social Security number and the passwords from her healthcare logins were found on the dark web. Plaintiff Leffers estimates she spent significant time responding to the Data Breach by researching the Data Breach, freezing her credit at the major credit bureaus, and contacting Experian about a suspicious entry on her credit report. Plaintiff Leffers signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

48. Prior to the Data Breach, Plaintiff Leffers had never experienced any type of fraud in her banking and credit card history. Plaintiff Leffers is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Leffers stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise

be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

49. **Plaintiff M.O. is a citizen of Illinois** residing in Chicago, Illinois. Plaintiff M.O. received a notice letter from Defendants dated September 3, 2023. On or about October 14, 2024, he learned from Credit Karma that on two separate occasions someone tried to access "his" Credit Karma account. But M.O. is not a Credit Karma user. Since August 2024 he has experienced unauthorized charges on his credit and debit cards on four different occasions, totaling about $200 altogether. Since February 2024, M.O. has also observed an uptake in spam telephone calls. Plaintiff M.O. estimates that he has spent about thirty hours responding to the Data Breach by fielding spam phone calls, monitoring his credit card accounts, and seeking reimbursement from his credit card company for unauthorized charges. Plaintiff M.O. continues to review his accounts for fraud.

50. Prior to the Data Breach, Plaintiff M.O. had never experienced any type of fraud in his banking and credit card history. Plaintiff M.O. is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff M.O. stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts. Plaintiff M.O. is distressed by the exposure of his PHI.

51. M.O. is HIV positive, and he is keenly aware of the stigma surrounding HIV. M.O. is deeply concerned about the release of this information against his consent and is particularly worried about the potential impact on his employment prospects and his relationships in his community.

52. **Plaintiff Joshua Lowe is a citizen of Indiana** residing in North Vernon, Indiana. Plaintiff Lowe received a notice letter from Defendants dated September 3, 2024. Since receiving notice, Plaintiff Lowe has experienced: (1) fraudulent charges on his credit and debit cards and bank accounts; (2) attempts at loans being opened in his name; (3) notifications that attempts to gain access to his accounts have been made; (4) increases in spam and phishing attempts; and (5) interruptions in utilities. Plaintiff Lowe estimates he spent about forty hours responding to the Data Breach by contacting the major credit bureaus to have his credit frozen, monitoring accounts for and investigating suspicious activity, and contacting banks, credit card companies, and other vendors about suspicious activity. Plaintiff Lowe estimates he has incurred $2,000 in out-of-pocket costs responding to the Data Breach by traveling to branches of his bank, paying for overdraft fees incurred through the fraud, and having utilities turned back on after they were shut off.

53. Prior to the Data Breach, Plaintiff Lowe had never experienced any type of fraud in his banking and credit card history. Plaintiff Lowe is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Lowe stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise

be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

54. **Plaintiff Rene Sims is a citizen of Indiana** residing in Munster, Indiana. Plaintiff Sims received a notice letter from Defendants dated August 5, 2024. On or about October 28, 2024, she learned that her Social Security number was found on the dark web. Plaintiff Sims estimates she spent about 5 hours responding to the Data Breach by researching the extent of the Data Breach and monitoring her accounts for suspicious and fraudulent activity. Plaintiff Sims continues to monitor her accounts for suspicious and fraudulent activity.

55. Plaintiff Sims is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Sims stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

56. **Plaintiff Hailey Kleinheksel is a citizen of Iowa** residing in Pocahontas, Iowa. Plaintiff Kleinheksel received a notice letter from Defendants dated August 5, 2024. On or about March 2024, she started receiving between 100-200 spam emails per day. Additionally, Plaintiff Kleinheksel's prescription medication was delayed twice in or about February 2024. Plaintiff Kleinheksel estimates she spent about 50 hours responding to the Data Breach by changing passwords to all bank accounts, email accounts, personal

applications, and social media sites, and she started using biometrics and two-factor authentication when available. Plaintiff Kleinheksel estimates she has incurred $6 in out-of-pocket costs responding to the Data Breach by purchasing an identity tracker via Experian. As discussed above, Plaintiff Kleinheksel signed up for an Experian identity tracker in response to the Data Breach and continues to review her accounts for fraud.

57. Plaintiff Kleinheksel is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Kleinheksel stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

58. **Plaintiff Michelle Carter is a citizen of Kansas** residing in Scott City, Kansas. Plaintiff Carter received a notice letter from Defendants dated September 3, 2024. Since about February 2024, she has experienced an increase in spam calls, text messages, and e-mails. On or about September 20, 2024, she learned that after getting access to her Social Security number, an unauthorized party pretending to be from an Oklahoma eye doctor's office charged her VSP Vision Account. Plaintiff Carter has also been notified that her Personal Information was found on the dark web. Plaintiff Carter estimates she spent about 8 hours responding to the Data Breach by researching the Data Breach, contacting card issues and her banks to preemptively get new numbers issued, monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, and

contacting VSP Vision about the fraudulent charge on her account. Plaintiff Carter estimates she has incurred approximately one day's wages, totaling $180, in out-of-pocket costs as a result of the Data Breach, because she had to spend time making phone calls to address the fraud, causing her to miss time with her students. Plaintiff Carter signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

59. Plaintiff Carter is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Carter stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

60. **Plaintiff Marissa Hatfield is a citizen of Kentucky** residing in Louisville, Kentucky. Plaintiff Hatfield received a notice letter from Defendants in or around August 2024. On or about February 2024, unauthorized users attempted to withdraw varying amounts of money from her bank account, totaling up to $180. As a result of this, she was blocked by her bank several times and had to get five new credit cards issued. Since February 2024, Plaintiff Hatfield received over 4,000 spam emails and phone calls from loan companies, along with threatening e-mails containing a picture of her home. Plaintiff Hatfield was also notified that her Personal Information is on the dark web. Plaintiff Hatfield estimates she spent about five hundred hours responding to the Data Breach by contacting card issuers/banks to preemptively new numbers issued, monitoring accounts

for suspicious activity, investigating fraudulent/suspicious activity, contacting her bank about fraudulent/suspicious activity, and changing passwords for any accounts that contains her Personal Information. Plaintiff Hatfield estimates she incurred approximately $29 in out-of-pocket costs responding to the Data Breach by having new credit cards issued. Plaintiff Hatfield continues to review her accounts for fraud.

61. Plaintiff Hatfield is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Hatfield stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

62. **Plaintiff Cedric Bonier is a citizen of Louisiana** residing in Bossier City, Louisiana. Plaintiff Bonier received a notice letter from Defendants dated August 5, 2024. On or about February 2024, he learned that unauthorized individuals opened an account at the Bank of Missouri and a Destiny Mastercard on his behalf without his knowledge. On or about February 2024, he also learned that an unauthorized user charged his Chase account for a total of $500 over the course of a few months. Out of the $500, he was only reimbursed $182. He also incurred three stop payment fees in the amount of $35 each. Plaintiff Bonier had to arrange for several new Chase debit cards to be issued. On or about February 2024, Plaintiff Bonier was also reissued an Applied Bank card because of the fraud he experienced. Since February 2024, Plaintiff Bonier receives approximately ten

spam calls per hour, between fifteen to twenty spam texts per day, and hundreds of spam emails on a regular basis. Plaintiff Bonier has been notified on several occasions that his Personal Information, including his Social Security Number and e-mail address, were found on the dark web. Plaintiff Bonier estimates he spent about fifteen hours responding to the Data Breach by researching the Data Breach, contacting major credit bureaus to freeze his credit, contacting card issuers/banks to preemptively get new numbers issued, monitoring accounts for suspicious activity, contacting banks and credit cards companies about fraudulent/suspicious activity, and changing his passwords for bank account and e-mail account. Plaintiff Bonier estimates he incurred $450 in out-of-pocket costs responding to the Data Breach in unreimbursed fraudulent charges, stop payment fees, and one-time payments for every new reissued payment card. Plaintiff Bonier continues to review his accounts for fraud.

63. Prior to the Data Breach, Plaintiff Bonier had never experienced any type of fraud in his banking and credit card history. Plaintiff Bonier is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Bonier stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

64. **Plaintiff Jan Merrill is a citizen of Maine** residing in Lewiston, Maine. Plaintiff Merrill received a notice letter from Defendants dated September 3, 2024. On or

about March 2024, she discovered fraudulent charges on her Bangor Savings debit card that involved monthly membership fees for a company she did not know. Additionally, in or about September 2024, she began receiving an influx of spam calls and texts, typically about 3 to 4 texts or calls each day. Plaintiff Merrill had to switch phone numbers because of the volume of spam she received. In or about September or October 2024, Plaintiff Merrill was notified that her Social Security number and other PII were found on the dark web. The breach has caused Plaintiff Merrill significant anxiety, concern about her loss of privacy, and fear over potential misuse of her sensitive information by cybercriminals. The increased stress has affected her physical and mental wellbeing. Plaintiff Merrill estimates she spent about 8 hours responding to the breach by researching the breach, contacting the three major credit bureaus to freeze her credit, contacting Lexis Nexis about the breach, and contacting her bank about the fraudulent charges on her debit card. Plaintiff Merrill estimates she has incurred about $50 in out-of-pocket costs responding to the breach by switching phone carriers to obtain a new phone number to reduce the spam she received. Plaintiff Merrill signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

65. Prior to the Data Breach, Plaintiff Merrill had never experienced any type of fraud in her banking and credit card history. Plaintiff Merrill is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Merrill stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise

be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

66. **Plaintiff Richard Seibert is a citizen of Maryland** residing in Maryland. Plaintiff Seibert received a notice letter from Defendants dated September 3, 2024. In or about June 2024, he received an increase in spam emails and phone calls. Plaintiff Seibert estimates he spent about fifteen hours responding to the Data Breach by researching the Data Breach and monitoring accounts for suspicious activity. Plaintiff Seibert continues to review his accounts for fraud.

67. Plaintiff Seibert is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Seibert stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

68. **Plaintiff Michael Paul is a citizen of Massachusetts** residing in Newton, Massachusetts. Plaintiff Paul received a notice letter from Defendants dated September 3, 2024. On or about August 2024, he learned that an unauthorized person attempted to open a Citibank account in his name. Plaintiff Paul estimates he spent about 1 hour responding to the Data Breach by contacting Citibank regarding the aforesaid unauthorized charge. Plaintiff Paul continues to review his accounts for fraud.

69. Plaintiff Paul is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Paul stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

70. **Plaintiff DeBorah Evans is a citizen of Michigan** residing in West Bloomfield, Michigan. Plaintiff Evans received a notice letter from Defendants dated September 3, 2024. In or about late August of 2024, she learned that an unauthorized user attempted to withdraw approximately $250 from her Huntington Bank account. In or about October 2024, Plaintiff Evans learned of another unauthorized attempt to withdraw approximately $250 from her Huntington Bank account. Due to these unauthorized attempts, she had to get her card reissued in both August and October of 2024, and had to go without access to her funds for approximately 6 days and 2 days respectively. Plaintiff Evans also experienced an increase in spam calls, emails, and texts. She estimates that she receives about 20-30 spam emails per day. Plaintiff Evans estimates that she spent about five (5) hours responding to the breach by researching the breach, reviewing her bank statements, contacting Huntington Bank to get new card numbers issued, monitoring her accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Evans continues to review her accounts for fraud.

71. Prior to the Data Breach, Plaintiff Evans had never experienced any type of fraud in her banking and credit card history. Plaintiff Evans is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Evans stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

72. **Plaintiff Lisa Brooks is a citizen of Minnesota** residing in Crystal, Minnesota. Plaintiff Brooks received a notice letter from Defendants dated September 3, 2024. On or about February 2024, she received an increase in spam emails and phone calls, including spam emails every other day and approximately two spam phone calls per week. On or about July 17, 2024, Plaintiff Brooks learned that her Personal Information, including her Social Security Number, was found on the dark web. Plaintiff Brooks estimates she spent about five hours responding to the Data Breach by contacting credit bureaus to freeze her credit, monitoring her accounts for suspicious activity, and changing passwords for all her accounts. Plaintiff Brooks continues to review her accounts for fraud.

73. Prior to the Data Breach, Plaintiff Brooks had never experienced any type of fraud in her banking and credit card history. Plaintiff Brooks is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Brooks stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the

mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

74. **Plaintiff David Powers is a citizen of Minnesota** residing in Little Canada, Minnesota. Plaintiff Powers received a notice letter from Defendants dated August 5, 2024. On or about October 2024, he learned his Personal Information was found on the dark web. Additionally, he has experienced an increase in spam calls and texts, including 5-6 calls and 50 text messages per week. Plaintiff Powers estimates he has spent between 15-20 hours responding to the Data Breach by monitoring his accounts for suspicious activity, changing all of his passwords, and researching the Data Beach. Plaintiff Powers continues to review his accounts for fraud.

75. Prior to the Data Breach, Plaintiff Powers had never been notified that his information was on the dark web. He is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Powers stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

76. **Plaintiff Roxanne Allen is a citizen of Minnesota** residing in Minneapolis, Minnesota. Plaintiff Allen had no knowledge of Defendant Change Healthcare, nor that her personal data was retained by Defendants. Plaintiff Allen received a notice letter from

Defendants dated September 3, 2024. On or about September 2024, she learned through her credit monitoring services that her Personal Information was found on the dark web. Shortly after, in or around September 2024, Plaintiff Allen began experiencing a substantial increase in suspicious email spam, many with health-related topics in the subject line. She receives on average 100+ spam emails each day, often identically sent to two email accounts requiring multiple daily cleanups. Plaintiff Allen believes the increase in suspicious spam calls to be an attempt to secure additional personal data and/or information from or about her. In or around March 2024, Plaintiff Allen experienced a delay in filling prescription medication, a problem she never had before the Data Breach. The Data Breach has caused Plaintiff Allen stress and anxiety about the compromise of her data; as a cancer patient now in remission, Plaintiff Allen is particularly concerned about the exposure of her sensitive medical information. Plaintiff Allen estimates she has spent between 30 and 45 hours to date responding to the Data Breach by shielding spam and suspicious phone calls, researching and responding to the Data Breach, including contacting her credit company to freeze her credit cards, invoking fraud alerts on her credit reporting accounts, and monitoring her accounts for suspicious activity. Plaintiff Allen estimates she has incurred $6.99 in monthly out-of-pocket costs responding to the breach by paying for continued AOL security and help desk assistance. Plaintiff Allen signed up for the IDX credit monitoring offered by Defendants and continues to review her accounts for fraud.

77. Prior to the Data Breach, Plaintiff Allen had never experienced any type of fraud in her banking and credit card history. Plaintiff Allen worked in financial services

technology and is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Allen stores any and all documents containing PII or PHI in a secure location and destroys via shredder any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts, which she closely monitors.

78. **Plaintiff Patricia Baggett is a citizen of Mississippi** residing in Wesson, Mississippi. Plaintiff Baggett received a notice letter from Defendants dated September 3, 2024. Around May or June of 2024, Plaintiff Baggett learned that someone had fraudulently accessed her Freshmart (CheckPlus) banking account and entered $8,000 into the account. She learned that the fraudsters were creating large loans through Upstart loans from her account. Plaintiff Baggett estimates she spent about 40-50 hours responding to the Data Breach by researching the extent of the Data Breach, monitoring her bank accounts, investigating fraudulent activity in her accounts, contacting her bank, the police, and reporting to the Financial Trade Commission. Plaintiff Baggett estimates she has incurred $600 in out-of-pocket overdraft fees from the perpetrator's fraudulent activity. Plaintiff Baggett enrolled in TransUnion's (JustWatch) credit and identity theft monitoring services and continues to review her accounts for fraud.

79. Prior to the Data Breach, Plaintiff Baggett had never experienced any type of fraud in her banking and credit card history. Plaintiff Baggett is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI

over the internet or any other unsecured source. Plaintiff Baggett stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

80. **Plaintiff Kenya Jones is a citizen of Missouri** residing in Florissant, Missouri. Plaintiff Jones received a notice letter from Defendants dated September 3, 2024. She has experienced several unauthorized charges. For example, on or about August 2024, Plaintiff Jones learned of an unauthorized charge on her Bank of America account. Plaintiff Jones also learned that her Personal Information was on the dark web. Plaintiff Jones estimates she spent about 40 hours responding to the Data Breach by monitoring her account for fraudulent activity, investigating suspicious charges, contacting Bank of America to obtain a new card, and communicating with the credit bureaus to freeze her credit. Plaintiff Jones continues to review her accounts for fraud.

81. Plaintiff Jones is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Jones stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

82. **Plaintiff Edwin Hoag is a citizen of Missouri** residing in Springfield, Missouri. Plaintiff Hoag received a notice letter from Defendants dated September 3, 2024. Plaintiff Hoag estimates he spent about 3 hours responding to the Data Breach by investigating the Data Breach and contacting the three major credit bureaus to freeze his credit. Since the Data Breach, Plaintiff Hoag has been notified that his Personal Information was found on the dark web. Plaintiff Hoag estimates he has incurred $25 in out-of-pocket costs responding to the Data Breach by purchasing "Incognito" to remove his Personal Information from the dark web. Plaintiff Hoag continues to review his accounts for fraud.

83. Prior to the Data Breach, Plaintiff Hoag had never experienced any type of fraud in his banking and credit card history. Plaintiff Hoag is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Hoag stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

84. **Plaintiff Richard Schwalbe is a citizen of Montana** residing in Big Sky, Montana. Plaintiff Schwalbe received a notice letter from Defendants dated August 5, 2024. Plaintiff Schwalbe estimates he spent about 10 hours responding to the Data Breach by researching the extent of it and contacting legal representation. Plaintiff Schwalbe is

enrolled in his bank's (Discover) credit and identity theft monitoring service and continues to review his accounts for fraud.

85. Prior to the Data Breach, Plaintiff Schwalbe had never experienced any type of fraud in his banking and credit card history. Plaintiff Schwalbe is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Schwalbe stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

86. **Plaintiff Delmar Kentner is a citizen of Nebraska** residing in Allen, Nebraska. Plaintiff Kenter received a notice letter from Defendants. Plaintiff Kentner estimates he spent about 20 hours responding to the Data Breach by freezing his credit, monitoring credit accounts for suspicious activity, and researching the Data Breach. Plaintiff Kentner estimates he has incurred around $10 in out-of-pocket costs responding to the Data Breach by sending a written notice to a credit reporting service. Plaintiff Kentner has frozen his accounts at the three main credit reporting agencies, Experian, TransUnion, and Equifax, enrolled in a credit monitoring service and uses the most extensive protection available against unauthorized access to all his accounts of whatever nature and continues to review his accounts for fraud.

87. Prior to the Data Breach, Plaintiff Kentner had never experienced any type of fraud in his banking and credit card history. Plaintiff Kentner is very careful about

sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Kentner stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

88. **Plaintiff Dawn Duncan is a citizen of Nevada** residing in Crystal, Nevada. Plaintiff Duncan received a notice letter from Defendants dated September 3, 2024. On or about June 2024, she discovered fraudulent charges on her credit card. Around the same time, Plaintiff Duncan began receiving an influx of healthcare-related phishing emails; she estimates that she receives 100-200 spam emails each week. Additionally, Plaintiff Duncan received several threatening emails addressing her by name and stating they would expose compromising photos of her if she if she did not pay between $1,000 to $5,000. Plaintiff Duncan has also received numerous junk emails mentioning a "Patrick Stevens" and a "Myhretta Gray," both unknown individuals to Plaintiff Duncan. These emails state they owe money to PayPal and are trying to collect payments from $299-$699. Plaintiff Duncan estimates she spent about 60 hours responding to the Data Breach by researching the Data Breach, notifying her bank about the Data Breach, contacting the major credit bureaus to put a fraud alert on her account, contacting the major credit bureaus to put a freeze on her credit account investigating fraudulent charges on her credit card, and cleaning spam emails out of her email account. Plaintiff Duncan signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

89. Prior to the Data Breach, Plaintiff Duncan had never experienced any type of fraud in her banking and credit card history. Plaintiff Duncan is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Duncan stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

90. **Plaintiff Rosa Rubera is a citizen of New Hampshire** residing in Manchester, New Hampshire. Plaintiff Rubera received a notice letter from Defendants dated September 3, 2024. Since the Data Breach, there have been numerous fraudulent attempts to access her financial accounts, she has experienced an increase in spam/phishing calls, a fraudulent Verizon account was opened using her PII, and she has received numerous alerts that her PII and PHI were found on the dark web. Plaintiff Rubera estimates she has spent approximately 50 hours responding to the Data Breach by researching the Data Breach, contacting Defendants about the Data Breach, contacting the major credit bureaus to freeze her credit, contacting card issuers and banks to preemptively get new numbers issued, monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, and contacting banks and credit card companies about fraudulent/suspicious activity. Plaintiff Rubera estimates she has incurred approximately $200 in out-of-pocket costs responding to the Data Breach by enrolling in credit monitoring

services in addition to the service offered by Defendants. Plaintiff Rubera signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

91. Prior to the Data Breach, Plaintiff Rubera had never experienced any type of fraud in her banking and credit card history. Plaintiff Rubera is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Rubera stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

92. **Plaintiff Matthew Loforese is a citizen of New Jersey**, residing in Sparta, New Jersey. Plaintiff Loforese received a notice letter from Defendants dated September 3, 2024. On or around March 2024, Plaintiff Loforese learned of an unauthorized $150 charge on his Capital One credit card. He also experienced several unauthorized transactions on his debit card in either March 2024 or April 2024, an email stating that his account was nearing overdraft status, and a fraud alert regarding the account. Around that same time, there was an unauthorized $75 charge on his Wells Fargo debit card. In or around November 2024, there was an unauthorized $300 charge on one of his credit cards (possibly via Synchrony Bank). Plaintiff Loforese has also experienced an increase in spam calls, emails, and texts (approximately 3-4/day), including emails stating he has outstanding toll fees, owes someone $4,000 via a PayPal transaction, and unsolicited offers to provide more of his prescription medications if he pays an unknown individual money.

Additionally, Plaintiff Loforese received a notification that his Personal Information was on the dark web on January 8, 2024. Plaintiff Loforese estimates he spent between 100-150 hours responding to the Data Breach by researching the Data Breach, changing passwords, reaching out to banks regarding fraudulent charges, monitoring his accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Loforese continues to review his accounts for fraud.

93. Plaintiff Loforese is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Loforese stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

94. **Plaintiff Carol Slack is a citizen of New Jersey** residing in Little Egg Harbor, New Jersey. Plaintiff Slack received a notice letter from Defendants dated September 23, 2024. Plaintiff Slack was notified that her email address was compromised via Capital One on May 26, 2024, she was notified by CreditWise of her Personal Information being found on the dark web on July 28, 2024, and she was notified by Capital One that her Personal Information was compromised again on August 3, 2024. Plaintiff Slack also experienced an increase in spam calls, text messages and mail since the Data Breach. She receives 7-8 spam phone calls and 3-4 spam text messages per day. For example, she received several phone calls from an unknown individual calling her

repeatedly, attempting to sell "mystical" products. Upon inquiring with one of these callers where they found her contact information, she was informed that they found it online in relation to a clinical trial she has no knowledge of and did not participate in. Plaintiff Slack estimates she spent about 80-100 hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Slack continues to review her accounts for fraud.

95. Plaintiff Slack is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Slack stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

96. **Plaintiff Rachael Schiller is a citizen of New Mexico** residing in Rio Rancho, New Mexico. Plaintiff Schiller received a notice letter from Defendants dated September 3, 2024. She has received an influx of spam since February 2024. For example, Plaintiff Schiller received a phishing email from Amazon Prime stating her credit card had expired and had to be updated, in addition to a text message claiming $745 was charged to her Amazon account. However, she does not have an Amazon Prime account in her name. Plaintiff Schiller estimates she receives between 3-5 spam messages per week. In the summer of 2024, she also received notice from Equifax and Identity Works that her Personal Information, including her Social Security number, was on the dark web. Plaintiff

Schiller estimates she spends between 1-1.5 hours a day responding to the Data Breach by reviewing and monitoring her bank statements, and changing passwords. Plaintiff Schiller continues to review her accounts for fraud.

97. Plaintiff Schiller is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Schiller stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

98. **Plaintiff Tristano Korlou is a citizen of New York** residing in Spencerport, New York. Plaintiff Korlou received a notice letter from Defendants dated September 23, 2024. On or about September 20, 2024, he received a letter from TransUnion alerting him that a Florida company made an inquiry on his credit file as part of an employment background investigation check. Plaintiff Korlou had not applied for any jobs and had never heard of the company listed in the letter. Additionally, since about June 2024, Plaintiff Korlou has had a significant uptick in spam emails and texts, typically receiving about 4-10 spam emails each day and spam 6-7 texts each week. These spam emails and texts often are addressed to him by name and include personal details. For example, in or about March 2025, Plaintiff Korlou received a spear-phishing email purportedly from a recruiter providing information about a marketing analyst position, and another email in or about January 2025 providing information about an associate marketing manager position;

Plaintiff Korlou previously spent more than two decades as a director in the marketing field. Plaintiff Korlou estimates he spent about 100 hours responding to the Data Breach by researching the Data Breach, freezing his credit at the three major credit bureaus, contacting a tertiary agency about the Data Breach, and evaluating texts, calls, and emails for phishing scams. Plaintiff Korlou continues to review his accounts for fraud.

99. Prior to the Data Breach, Plaintiff Korlou had never experienced any type of fraud in his banking and credit card history. Plaintiff Korlou is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Korlou stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

100. **Plaintiff Patricia Donadio is a citizen of New York** residing in Farmington, New York. Plaintiff Donadio received a notice letter from Defendants in September 2024. On or about October 2024, she learned that an unauthorized user attempted to spend over $2,000 from her Mercury bank account. Plaintiff Donadio also experienced an increase in spam/phishing calls and emails. Plaintiff Donadio estimates she spent about 10 hours responding to the Data Breach by researching the Data Breach, contracting credit bureaus to freeze her credit, contacting Mercury bank to resolve fraudulent attempts, monitoring her accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Donadio continues to review her accounts for fraud.

101. Prior to the Data Breach, Plaintiff Donadio had never experienced any type of fraud in her banking and credit card history. Plaintiff Donadio is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Donadio stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

102. **Plaintiff James Morgan is a citizen of North Carolina** residing in Leland, North Carolina. Plaintiff Morgan received a notice letter from Defendants dated September 3, 2024. On or about September 2024, he learned that an unauthorized user attempted to withdraw $3,300 from his Truist bank account. Plaintiff Morgan also experienced an increase in spam calls, emails, and texts. Plaintiff Morgan estimates he spent about 10 hours responding to the Data Breach by researching the Data Breach, contacting credit bureaus to freeze his credit, contacting Truist bank to close his account and get new bank account numbers issued, monitoring his accounts for suspicious activity, and investigating fraudulent/suspicious activity. Plaintiff Morgan continues to review his accounts for fraud.

103. Prior to the Data Breach, Plaintiff Morgan had never experienced any type of fraud in his banking and credit card history. Plaintiff Morgan is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Morgan stores any and all

documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

104. **Plaintiff Kaela Poitra is a citizen of North Dakota** residing in Minot, North Dakota. Plaintiff Poitra received a notice letter from Defendants dated September 3, 2024. On or about January 2025, she learned that there was an unauthorized charge of $19.99 on her SoFi debit card for a PURE Energy drink, an item she never buys. As a result of this, her debit card was put on hold. Since about February 2024, Plaintiff Poitra experienced an increase in spam emails and phone calls. Specifically, she has been receiving spam calls from the "Motor Service Department" regarding vehicle coverage even though she has not owned a car in over 10 years. Plaintiff Poitra estimates she spent about 5 hours responding to the Data Breach by contacting SoFi about the unauthorized charge on her debit card, monitoring her accounts for suspicious activity, researching the Data Breach, and investigating fraudulent/suspicious activity. Plaintiff Poitra continues to review her accounts for fraud.

105. Plaintiff Poitra is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Poitra stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise

her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

106. **Plaintiff Autumn Abramczyk is a citizen of Ohio** residing in Wickliffe, Ohio. Plaintiff Abramczyk received a notice letter from Defendants dated September 3, 2024. On or about October 2, 2024, Plaintiff Abramczyk learned that her PII had been found on the dark web. In or about November 2024, Plaintiff Abramczyk discovered someone had fraudulently gained access to her online Walmart account and purchased something using her PayPal account. Then, a few days later, Plaintiff Abramczyk caught a fraudulent charge on her debit card after receiving a text alert from her bank about a purchase she had not made. Plaintiff Abramczyk estimates she has incurred $30.81 in monthly out-of-pocket costs responding to the Data Breach by continuing to pay for her LifeLock by Norton credit-monitoring service. Plaintiff Abramczyk estimates she spent about 20-30 hours responding to the Data Breach by researching the Data Breach and contacting Defendants, her health insurance company, and her healthcare providers about the Data Breach. Plaintiff Abramczyk continues to review her accounts for fraud.

107. Prior to the Data Breach, Plaintiff Abramczyk had never experienced any type of fraud in her banking and credit card history. Plaintiff Abramczyk is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Abramczyk stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that

could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

108. **Plaintiff Anna Griffith is a citizen of Ohio** residing in Newark, Ohio. Plaintiff Griffith received a notice letter from Defendants dated September 23, 2024. In or about September 2024, she was locked out of her Huntington Bank card and was unable to access her account online. An unknown and unauthorized individual had added a phone number and email to her online banking information. As a preventative measure, Plaintiff Griffith closed the account and opened a new one. Additionally, Plaintiff Griffith learned that an unknown and unauthorized individual used a falsified driver's license reflecting her name and signature to withdraw $9,600 from her Huntington Bank account at Huntington Bank's Michigan branch. On January 7, 2025, Plaintiff Griffith learned of another unauthorized withdrawal from her checking account at the Detroit Tower branch of Huntington Bank in the amount of $6,000, in the same manner as the previous unauthorized withdrawal, which was successfully refunded by the bank on January 15, 2025. Further, Plaintiff Griffith had $2,600 transferred out of her account via Zelle by an unknown and unauthorized individual. She also received, and continues to receive, a significant amount of spam calls, emails, and text messages. Plaintiff Griffith estimates she spent about 21 hours responding to the Data Breach by researching the Data Breach, contacting the major credit bureaus to freeze her credit, contacting her financial institutions to preemptively get new cards issued, visiting the BMV to file a report to get a new driver's license, monitoring her accounts for suspicious activity, contacting her bank and/or credit card companies about fraudulent/suspicious activity, and contacting police department in Ohio and

Michigan. Plaintiff Griffith estimates she has incurred $280 in out-of-pocket costs in response to the Data Breach for prematurely withdrawing funds from her Huntington Bank certificate of deposit savings account and paying for anti-virus protection software for her mobile phone. Plaintiff Griffith continues to review her accounts for fraud.

109. Prior to the Data Breach, Plaintiff Griffith had never experienced any type of fraud in her banking and credit card history. Plaintiff Griffith is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Griffith stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

110. **Plaintiff Preslee Thorne is a citizen of Oklahoma** residing in Oklahoma City, Oklahoma. Plaintiff Thorne received a notice letter from Defendants dated September 3, 2024. On or about February 20, 2024, she experienced, and continues to experience, a significant uptick in spam texts, calls, and emails. Prior to February 20, 2024, Plaintiff Thorne received one or two spam calls, texts, or emails every two to three weeks. Now, Plaintiff Thorne receives multiple spam calls, texts, and emails per day. Additionally, Plaintiff Thorne had multiple medical claims rejected that would not normally be rejected and experienced significant delays in attempting to purchase her prescription medication. Plaintiff Thorne estimates she spent about 10 hours responding to the Data Breach by researching the Data Breach, contacting Defendants about the Data Breach, freezing her

credit, monitoring her accounts for suspicious activity, and contacting her financial institutions. Plaintiff Thorne estimates she has incurred $80 in out-of-pocket costs responding to the Data Breach by subscribing to BitDefender. This subscription fee increases to $100 after the initial discount period concludes. Plaintiff Thorne continues to review her accounts for fraud.

111. Prior to the Data Breach, Plaintiff Thorne had never experienced any type of fraud in her banking and credit card history. Plaintiff Thorne is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Thorne stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

112. **Plaintiff Robin Lanier is a citizen of Oregon** residing in Cottage Grove, Oregon. Plaintiff Lanier received a notice letter from Defendants dated August 5, 2024. On or about August 20, 2024, she learned that her email, phone number, and Social Security Number were detected on the dark web. Plaintiff Lanier estimates she spent about 10 hours responding to the Data Breach by researching the Data Breach and contacting Experian to freeze her credit. Plaintiff Lanier has responded to the Data Breach by researching the Data Breach, contacting major credit bureaus, like Experian, to freeze credit, and monitoring accounts for suspicious activity. Plaintiff Lanier uses Experian Credit Services and continues to review her accounts for fraud.

113. Plaintiff Lanier is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Lanier stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

114. **Plaintiff Ashley Harbon is a citizen of Pennsylvania** residing in Haverford, Pennsylvania. Plaintiff Harbon received a notice letter from Defendants dated July 29, 2024. On or about September 12, 2024, she learned that her Personal Information was found on the dark web and fell victim to a fake job interview from her increased spam emails and calls. Plaintiff Harbon estimates she spent about 10 hours responding to the Data Breach by monitoring and investigating accounts for fraudulent activity.

115. Plaintiff Harbon is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Harbon stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. Plaintiff Harbon continues to review his accounts for fraud.

116. **Plaintiff Kim Kaehler is a citizen of Pennsylvania** residing in Harrisburg, Pennsylvania. Plaintiff Kaehler received a notice letter from Defendants dated September 3, 2024. She also received a notice letter from Defendants dated December 2, 2024, addressed to the estate of her late mother, Lydia Peiffer. Ms. Peiffer passed away on or about August 12, 2017. Since the Data Breach, Plaintiff Kaehler has received an increase in spam calls and text messages. On or about March 2024, Plaintiff Kaehler filled her Forteo Injection pen prescription through CVS Specialty. Plaintiff Kaehler was enrolled in a patient assistance payment plan that lowered her copay to $4 per month. Unbeknownst to Plaintiff Kaehler, Defendants' Data Breach prevented her patient assistance payment plan from processing her March prescription correctly. Plaintiff Kaehler discovered this error in or around July 2024, when her copay assistance was declined. Plaintiff Kaehler was then informed her copay for her Forteo prescription would be about $2,717. Unable to pay this amount, Plaintiff Kaehler canceled the order and contacted her doctor to find an alternative. Plaintiff Kaehler received a prescription for a generic version of the Forteo pen in late July 2024. About 4 to 5 days after Plaintiff Kaehler began taking the generic prescription, she developed a rash. On or about September 7, 2024, Plaintiff Kaehler sought medical advice about the rash. She was told to temporarily stop taking the generic pen and to take Prednisone to try to stop the rash. Plaintiff Kaehler went through two total rounds of Prednisone to treat the rash before her doctor determined she was allergic to the generic version of Forteo. Plaintiff Kaehler had to go without any medication for her osteoporosis between September 2024 and January 4, 2025, when she finally received a Forteo pen prescription and patient assistance payment plan again. Additionally, in or around July and

August 2024, Plaintiff Kaehler received demands from CVS Specialty Pharmacy that she pay about $1,240 from March 2024, when CVS Specialty determined her patient assistance funds were exhausted. That amount is about 50% of Plaintiff Kaehler's current income, which consists of long-term disability and her pension. Plaintiff Kaehler spent significant time trying to fix the issue. On or about August 20, 2024, Plaintiff Kaehler was told that there was a possibility that she could get reimbursed for paying the balance through the Lilly Post Transaction Department. Plaintiff Kaehler declined to do so until, on or about August 26, 2024, she received a guarantee on or from a supervisor at Lilly that she would get reimbursed for the amount. Plaintiff Kaehler paid the amount on a credit card on or about August 28, 2024, and she received the reimbursement on or about September 5, 2024. Plaintiff Kaehler estimates she spent more than 40 hours responding to the breach by researching the breach; calling numerous pharmaceutical companies about the prescription bill; and working with her doctor to get switched to a different, cheaper alternative to Forteo. During a call to CVS Specialty Pharmacy, Plaintiff Kaehler was told the cost change was due to a problem with the patient assistance payment plan because of the Data Breach. Plaintiff Kaehler estimates she has incurred about $32 in out-of-pocket costs due to the breach, namely from the generic pens prescription copay and the copay for the two rounds of prednisone, as well as for the postage cost of mailing her claim form to the Savings Card Post-Transaction Reimbursement program. Plaintiff Kaehler continues to review her accounts for fraud.

117. Prior to the Data Breach, Plaintiff Kaehler had never experienced any type of fraud in her/his banking and credit card history. Plaintiff Kaehler is very careful about

sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Kaehler stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

118. **Plaintiff Sally Kirkpatrick is a citizen of Pennsylvania** residing in Erie, Pennsylvania. Plaintiff Kirkpatrick received a notice letter from Defendants dated September 3, 2024. On or about October 2, 2024, she learned that an unauthorized party had attempted to open an Indigo Bank account using the last name, "Trayer," a name she has not used since 2007. Plaintiff Kirkpatrick has also received notice that her Personal Information was found on the dark web. Additionally, Plaintiff Kirkpatrick experienced an increase in spam calls, emails, and texts. Plaintiff Kirkpatrick estimates she spent about 3 hours responding to the Data Breach by freezing her credit and contacting Indigo Bank to dispute the unauthorized account. Plaintiff Kirpatrick has signed up for the credit monitoring offered by Defendants.

119. Prior to the Data Breach, Plaintiff Kirkpatrick had never experienced any type of fraud in her banking and credit card history. Plaintiff Kirkpatrick is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Kirkpatrick stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that

could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

120. **Plaintiff Tess Bussick was a citizen of Rhode Island** residing in Rhode Island at the time of the Data Breach. Plaintiff Bussick received a notice letter from Defendants dated September 3,2024. On or about April 20, 2024, she learned (via letter) that someone had opened a Charles Schwab account in her name and tried to deposit a $15,000 check. Charles Schwab subsequently tried to impose a $25 fee because the check was invalid. When Plaintiff Bussick called Chales Schwab in early May 2024, she learned the account had been locked. Plaintiff Bussick received another letter approximately 2 days later stating she had an outstanding balance of $25. Additionally, on July 6, 2024, Plaintiff Bussick received a text from Fidelity Bank stating that someone had opened an account in her name. She called Fidelity Bank and learned that the unauthorized person had used her name, Social Security Number, prior Rhode Island address, and other Personal Information to open the checking account. On July 29, 2024, an unauthorized party attempted to open a Chase account in Plaintiff Bussick's name, but as her credit was frozen, the attempt was unsuccessful. A USAA account was also opened in Plaintiff Bussick's name on March 12, 2024. In fact, someone named Tyler Falish from Kroll in New York called her and then her dad, claiming that someone deposited a $4,000 check from his client to the fraudulent account. Plaintiff Bussick estimates she spent about 50 hours responding to the Data Breach by researching the Data Breach, contacting all three major credit bureaus to freeze her credit, contacting the above-referenced banks regarding the fraudulent accounts, monitoring her accounts for suspicious activity, and investigating any fraudulent activity.

Moreover, Plaintiff Bussick worked closely with a private investigator from July 2024-September 2024 regarding the fraudulent activity. Plaintiff Bussick estimates she has incurred $50 in out-of-pocket costs responding to the Data Breach by paying for a police report and on gasoline used in traveling to and from the police station and USAA Bank, and enrolling in an Experian credit monitoring service. Plaintiff Bussick has also signed up for the credit monitoring offered by Defendants and she continues to review her accounts for fraud.

121. Prior to the Data Breach, Plaintiff Bussick had never experienced any type of fraud in her banking and credit card history. Plaintiff Bussick is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Bussick stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

122. **Plaintiff Lori Tynch is a citizen of South Carolina** residing in Nichols, South Carolina. Plaintiff Tynch received a notice letter from Defendants dated September 3, 2024. Since February 20, 2024, she has experienced approximately 27 fraudulent transactions on her Amazon account, totaling about $1,000. She also received, and continues to receive, an excessive amount of spam calls, emails, and texts. Plaintiff Tynch estimates she spent about 3.5 hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity, investigating

fraudulent/suspicious activity, and contacting various financial institutions about fraudulent/suspicious activity. Plaintiff Tynch continues to review her accounts for fraud.

123. Prior to the Data Breach, Plaintiff Tynch had never experienced any type of fraud in her banking and credit card history. Plaintiff Tynch is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Tynch stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

124. **Plaintiff Polly Rush is a citizen of South Dakota** residing in Aberdeen, South Dakota. Plaintiff Rush received a notice letter from Defendants dated August 5, 2024. On or about August 29, 2024, she learned through CreditWise that her Personal Information, including her Social Security number, was on the dark web. Plaintiff Rush estimates she spent about 20 hours responding to the Data Breach by researching the Data Breach, contacting her banks, and communicating with CreditWise regarding her PII being found on the dark web. Plaintiff Rush is enrolled in CreditWise monitoring and continues to review her accounts for fraud.

125. Prior to the Data Breach, Plaintiff Rush had never experienced any type of fraud in her banking and credit card history. Plaintiff Rush is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Rush stores any and all documents

containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

126. **Plaintiff Anna Lovell is a citizen of Tennessee** residing in Chattanooga, Tennessee. Plaintiff Lovell received a notice letter from Defendants dated August 5, 2024. After the Data Breach, she began receiving fraudulent calls and spam trying to obtain further access and information to her accounts. Plaintiff Lovell estimates she spent at least 5 hours responding to the Data Breach by researching the Data Breach, investigating suspicious activity on her accounts, and contacting banks to shut down cards and accounts. Plaintiff Lovell continues to review her accounts for fraud.

127. Prior to the Data Breach, Plaintiff Lovell had never experienced any type of fraud in her banking and credit card history. Plaintiff Lovell is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Lovell stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

128. **Plaintiff Christina Estep is a citizen of Texas** residing in Conroe, Texas. Plaintiff Estep received a notice letter from Defendants dated August 5, 2024. On or about February 20, 2024, she began to receive multiple medical bills fraudulently charged to her

accounts. On or about March 19, 2024, Plaintiff Estep suffered a stress-induced transient ischemic attack ("TIA") because of stress and fear related to this Data Breach. Since April 2024, Plaintiff Estep has had five credit cards opened in her name by unknown and unauthorized individuals. Additionally, she has received utility bills referencing a residence in Ohio. She also experienced, and continues to experience, a significant increase in spam calls, texts, and emails. Further, Plaintiff Estep has had three medical claims denied on March 8, 2024, October 24, 2024, and November 13, 2024. During the first four months following the Data Breach, Plaintiff Estep estimates she spent several hours a day responding to the Data Breach, contacting the major credit bureaus to freeze her credit, contacting card issuers and/or financial institutions to preemptively get new card numbers issued, and contacting various financial institutions about fraudulent/suspicious activity. Additionally, she spent numerous hours on the phone with the Federal Trade Commission, her local police department, and the Department of Motor Vehicles to secure a new license. Further, since the Data Breach, her credit score has plummeted from 650 to 440. Plaintiff Estep estimates she has incurred $500 in out-of-pocket costs responding to the Data Breach by filing police reports with the local police, purchasing monthly subscriptions to credit monitoring services and other security services, and/or research services such as KickOff, Ai Dudly, and Lexington Law. Plaintiff Estep continues to review her accounts for fraud.

129. Prior to the Data Breach, Plaintiff Estep had never experienced any type of fraud in her banking and credit card history. Plaintiff Estep is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Estep stores any and all documents

containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

130. **Plaintiff Alfred Williams, Sr. is a citizen of Texas** residing in Corpus Christie, Texas. Plaintiff Williams received notice letters from Defendants dated August 5, 2024, and September 3, 2024. On or about June 30, 2024, an unauthorized $1,400 payment from New York appeared on his credit card. Since the Data Breach, Plaintiff Williams has also observed a significant uptick in spam phone calls and text messages. Plaintiff Williams estimates he has spent about 12 to 14 hours responding to the Data Breach by contacting his credit card companies to ensure that they were aware his information was compromised, contacting his credit card company to resolve the fraudulent charges, investigating fraud, and monitoring his accounts for suspicious activity. Plaintiff Williams continues to review his accounts for fraud.

131. Prior to the Data Breach, Plaintiff Williams had never experienced any type of fraud in his banking and credit card history. Plaintiff Williams is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Williams stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

132. **Plaintiff Angela Johnson is a citizen of Utah** residing in Clinton, Utah. Plaintiff Johnson received a notice letter from Defendants dated September 23, 2024. Since March 2024, she has received, and continues to receive, large amounts of spam calls, texts, and emails. Plaintiff Johnson estimates she spent about 6 hours responding to the Data Breach by researching the Data Breach, monitoring her accounts for suspicious activity, and changing the passwords to her financial and social media accounts. Plaintiff Johnson continues to review her accounts for fraud.

133. Plaintiff Johnson is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Johnson stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise Plaintiff Johnson identity and financial accounts. Moreover, Plaintiff Johnson diligently chooses unique usernames and passwords for her various online accounts.

134. **Plaintiff Trudy Agres is a citizen of Vermont** residing in Bennington, Vermont. Plaintiff Agres received a notice letter from Defendants dated October 30, 2024. Since the Data Breach, Plaintiff Agres has experienced an increase in spam emails and calls, often about 4 to 5 calls each week. Plaintiff Agres estimates she spends approximately one hour each day responding to the Data Breach by researching the Data Breach, contacting the major credit bureaus, contacting her banks and card issuers, and monitoring her accounts and credit report. Plaintiff Agres signed up for the credit monitoring offered by Defendants and continues to review her accounts for fraud.

135. Prior to the Data Breach, Plaintiff Agres had never experienced any type of fraud in her banking and credit card history. Plaintiff Agres is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Agres stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

136. **Plaintiff Leigh Thompson (Tom) Hanes is a citizen of Virginia** residing in Manakin Sabot, Virginia. Plaintiff Hanes received a notice letter from Defendants dated September 3, 2024. On or about September 20, 2024, he learned that he was a victim of the Data Breach. He also experienced a significant increase in spam calls and e-mails. Plaintiff Hanes estimates he spent about 7 hours responding to the Data Breach by researching the Data Breach, contacting Defendants regarding the Data Breach, and monitoring various accounts for suspicious activity. Plaintiff Hanes continues to review his accounts for fraud.

137. Plaintiff Hanes is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Hanes stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his

identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

138. **Plaintiff J'Andre Ivory is a citizen of Washington** residing in Yelm, Washington. Plaintiff Ivory received a notice letter from Defendants dated September 3, 2024. On or about August 2024, he began experiencing an increase in suspicious spam telephone calls using his compromised Personal Information that he believes to be an attempt to secure additional information from or about him. Additionally, around the same time, Plaintiff Ivory learned that his personal email for the first time began requiring a code to log in, signaling someone is trying to access his account. Plaintiff Ivory also learned through his Discover Credit Monitoring that his Personal Information, including Social Security number, was found on the Dark Web. Plaintiff Ivory estimates he spent about 60 hours responding to the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and changing passwords to email and other personal accounts. Plaintiff Ivory continues to review his accounts for fraud.

139. Plaintiff Ivory is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Ivory stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

140. **Plaintiff Harry Knopp is a citizen of West Virginia** residing in Ripley, West Virginia. Plaintiff Knopp received a notice letter from Defendants dated September 3, 2024. On or about August 2024, he learned that his bank caught someone trying to access his account to make fraudulent charges. Plaintiff Knopp estimates he spent about 10 to 15 hours responding to the Data Breach by researching the Data Breach, contacting his banks, and investigating fraudulent and suspicious activity on his accounts. Plaintiff Knopp signed up for the credit monitoring offered by Defendants and continues to review his accounts for fraud.

141. Prior to the Data Breach, Plaintiff Knopp had never experienced any type of fraud in his banking and credit card history. Plaintiff Knopp is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Knopp stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

142. **Plaintiff Mark Wetzel is a citizen of West Virginia** residing in Martinsburg, West Virginia. Plaintiff Wetzel received a notice letter from Defendants dated September 3, 2024. After the Data Breach, he was notified by AT&T, American Express, Bank of America, Wells Fargo, and Discover that unauthorized parties opened accounts in those respective companies on his behalf. He also learned that an unauthorized party was attempting to apply for a Walmart card using his address. Since February 2024, Plaintiff

Wetzel has experienced an increase in spam e-mails, text messages, and phone calls. Specifically, he receives 5 spam text messages, 50 spam phone calls, and 100 spam e-mails per week. The sheer volume of spam he receives on a regular basis causes his phone to slow down if he does not delete it from his phone. Plaintiff Wetzel estimates he spent about 100 hours responding to the Data Breach by researching the Data Breach, monitoring accounts for fraudulent activity, and investigating suspicious/fraudulent activity. Plaintiff Wetzel continues to review his accounts for fraud.

143. Plaintiff Wetzel is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Wetzel stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

144. **Plaintiff Luke Anderson is a citizen of Wisconsin** residing in Porterfield, Wisconsin. Plaintiff Anderson received a notice letter from Defendants dated September 3, 2024. On or about February 2024, an unauthorized party attempted to apply for a vehicle loan in his name and tried to access his credit report. On or about February 2024, Plaintiff Anderson learned that someone in Florida was using his Discover credit card at a parking garage and had to have his credit card reissued resulting in the inability to access his funds for 7 days. Since February 2024, Plaintiff Anderson has experienced an increase in spam texts and calls—he receives approximately 5 spam text messages and phone calls per day.

On or about October 2024, an unauthorized party accessed his Sirius XM account. As a result, he got a letter in the mail notifying him that his trial period for his Mercedes was ending, when in reality, he neither owns a Mercedes nor did he sign up for a trial period. On or about November 2024, Plaintiff Anderson learned that an unauthorized party accessed his Progressive vehicle insurance account and added an unknown vehicle to his insurance account. Plaintiff Anderson estimates he spent about 20 hours responding to the Data Breach by getting in touch with Progressive and Sirius XM to resolve the fraudulent access to his accounts, getting a new Discover card reissued, deleting the spam texts he constantly receives, and monitoring his accounts for fraudulent activity. Plaintiff Anderson continues to review his accounts for fraud.

145. Prior to the Data Breach, Plaintiff Anderson had never experienced any type of fraud in his banking and credit card history. Plaintiff Anderson is very careful about sharing his own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Anderson stores any and all documents containing PII or PHI in a secure location and destroys any documents he receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

146. **Plaintiff Lauren Fossen is a citizen of Wyoming** residing in Laramie, Wyoming. Plaintiff Fossen received a notice letter from Defendants dated August 5, 2024. On or about July 2024, she learned that an unauthorized party had obtained two federal student loans in her name, totaling $3,300. Plaintiff Fossen has also received notice that

her Personal Information was found on the dark web. Additionally, Plaintiff Fossen experienced an increase in spam calls, receiving approximately 7-10 per week. Plaintiff Fossen estimates she spent about 10 hours responding to the Data Breach by researching the Data Breach, contacting credit bureaus to freeze her credit, contacting Federal Student Aid, Central Research, Inc. (a company that handles student loans), law enforcement, and the FTC regarding the above-referenced loans, and monitoring her accounts for suspicious activity. Plaintiff Fossen estimates she has incurred $89.95 in out-of-pocket costs responding to the Data Breach by enrolling in LifeLock (an annual membership). Plaintiff Fossen continues to review her accounts for fraud and dispute the previously mentioned fraudulent federal student loans.

147. Plaintiff Fossen is very careful about sharing her own PII and PHI and has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source. Plaintiff Fossen stores any and all documents containing PII or PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

II. Defendants

A. UHG

148. Defendant UnitedHealth Group "is a vertically integrated healthcare company" comprised of United Healthcare ("UHC"), a health insurance company, and

three Optum divisions: Optum Health, OptumInsight, and Optum Rx. [11] UHG "is a health care leviathan" that, in 2023, generated $324 billion in revenue, making it the fifth largest company in America.[12] UHG is incorporated in Delaware and headquartered in Minnetonka, Minnesota.[13]

B. Optum

149. Defendant Optum, Inc. ("Optum") is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota. Optum is a subsidiary of UHG and operates three main healthcare-related businesses: Optum Health, Optum RX, and Optum Insight.

C. Optum Insight

150. Optum Insight is a Delaware corporation with its principal place of business at 1 Optum Circle, Eden Prairie, MN 55344.

151. Optum Insight is the data analytics and technology arm of the UHG organization. It serves four types of customers: (1) payors (insurers and self-funded benefit providers), (2) state governments, (3) healthcare providers, and (4) life sciences companies

[11] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 3 (D.D.C. Sept. 7, 2022).

[12] *Opening Statement Testimony of Senator Ron Wyden*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf at 1 (last visited Nov. 26, 2024).

[13] *UHG's Articles of Incorporation*, UnitedHealth Group, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/About/UNH-Certificate-Of-Incorporation.pdf (last visited Nov. 27, 2024).

that develop and manufacture drugs, devices, and medical treatments. Optum Insight is also a technology supplier to its sister company, the insurer United Healthcare.

152. "Optum Insight provides technology-enabled services built on the foundation of our health care focus, advanced analytics and cross-industry connections to help customers reduce costs, better manage risk and quality, and grow revenue." [14]

153. In January 2021, UHG agreed to purchase Change Healthcare for approximately $13 billion.[15] In October 2022, following a DOJ antitrust investigation into the merger and a trial ultimately approving the merger, UHG finalized its acquisition of Change. Change Healthcare and was merged with Optum Insight.[16]

154. After combining the Change Healthcare and Optum Insight businesses in October 2022 under Change Healthcare's CEO, Neil de Crescenzo, UHG CEO Andrew Witty explained that Optum Insight and Change Healthcare were combining to create

[14] [14] *Optum*, UnitedHealth Group, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2022/conference/UHG_IC_22_Optum_Consolidated.pdf (last visited Jan. 14, 2025).
[15] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 9 (D.D.C. Sept. 21, 2022).
[16] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 11 and 18 (D.D.C. Sept. 7, 2022); James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, Forbes (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.

"more effective and simple experiences for consumers, payers and care providers while lowering costs across the health system."[17]

155. At the same time, UHG's CFO explained that UHG would be spending $100M to integrate Change Healthcare into Optum Insight. The integration was expected to bring in $800M in revenue to the Optum Insight organization in the fourth quarter of 2022.[18]

156. By the fourth quarter of 2022, UHG stated that Change Healthcare and Optum Insight had been integrated and were "executing on the synergies of this combination."[19]

D. Change Healthcare

157. Defendant Change Healthcare is a Delaware corporation with its principal place of business in Nashville, Tennessee. Founded in 1996, Change Healthcare provides data solutions to health insurers and providers to facilitate clinical decision making and payment processing across the healthcare industry.[20] In 2017, Change Healthcare entered into a joint venture with McKesson Corporation's Technologies Solutions Division to form

[17] *UnitedHealth Group (UNH) Q3 2022 Earnings Call Transcript*, Motley Fool (Oct. 14, 2022), https://www.fool.com/earnings/call-transcripts/2022/10/14/unitedhealth-group-unh-q3-2022-earnings-call-trans/.

[18] *Id.*

[19] *UnitedHealth Group (UNH) Q4 2022 Earnings Call Transcript*, Motley Fool (Jan. 13, 2023), https://www.fool.com/earnings/call-transcripts/2023/01/13/unitedhealth-group-unh-q4-2022-earnings-call-trans/.

[20] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 45 (D.D.C. Sept. 7, 2022).

the healthcare technology company that existed at the time of its merger with Optum Insight in 2022.[21]

158. Change Healthcare operates a computer network that facilitates data transfers among healthcare system participants, including physicians, pharmacists, and insurers. Through its suite of software, analytics, technology-enabled services, and network solutions, it purports to enhance clinical decision-making, and simplify billing, collection, and payment processes.

159. In its press release announcing the acquisition, Optum stated that its combination with Change Healthcare would "connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients." The U.S. Dept. of Justice and the American Hospital Association ("AHA") presciently cast doubts on those claims, highlighting the dangers of concentrating essential healthcare services and processes in UHG and Change Healthcare.[22]

160. Generally, payments for healthcare services in the United States proceed in the following fashion: health insurers like UHC, also known as "payers," pay medical claims submitted by caregivers, also known as "providers."[23] The process begins with a patient seeking care from a provider, who confirms insurance coverage before providing

[21] *Id.* at 46.
[22] *Testimony of AHA at Hearing "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack,"* House Committee on Energy and Commerce (Apr. 16, 2024), https://www.aha.org/system/files/media/file/2024/04/24-04-29-AHALTRtoEandConUHG-webwattachment.pdf at 2-3 (last visited Nov. 27, 2024).
[23] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 1-2 (D.D.C. Sept. 21, 2022).

treatment. The provider then treats the patient.[24] The provider then submits a claim to a payer so that the provider can be compensated for treating the patient.[25] Prior to paying the provider, the payer evaluates the submitted claim to determine how much, if any, it should pay the provider for the services rendered.[26] The payer then sends the provider an Electronic Remittance Advice, or ERA, which outlines the claim, the allowable amounts paid or denied, that the practice uses to reconcile the patient's account balance,[27] and pays the provider the determined amount.[28] The provider then bills the patient for the appropriate amounts under their insurance plan, or the provider may appeal the determination of the payer.

161. The exchanges of information described above occur through Electronic Data Interchange ("EDI") clearinghouses, which serve as the "pipes" through which electronic transmission of claims, payment remittances, and other information are exchanged between payers and providers.[29] EDI clearinghouses are used by 95% of providers and by 99% of insurers.[30]

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.* at 3-4.
[30] *Id.*

162. EDI clearinghouse transactions are submitted in standardized transaction formats, which include a substantial amount of highly sensitive PII and PHI in order to effectuate revenue management, clinical decision making, and patient support. [31]

163. Change Healthcare's EDI clearinghouse, which includes a suite of revenue management, clinical, and patient support software, is called the Change Healthcare Platform ("Change Platform"). In theory, the standardized format of information in EDI clearinghouse transactions should enable clearinghouses, providers, and health insurers to be interoperable across the healthcare industry.[32] In practice, as evidenced by the immense disruption to claims processing following the Data Breach, that is not the case. This is largely because providers connect with the Change Platform either directly or indirectly via a third-party vendor or intermediary.[33] Some providers connect directly with Change Healthcare to access the Change Platform, while most providers use electronic health records ("EHR") or revenue cycle management ("RCM") vendors to establish an indirect connection to the Change Platform.[34] Providers and payers are able to transmit claims to clearinghouses for which they do not have a direct or indirect connection via "hops"

[31] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 53, 61 (D.D.C. Sept. 7, 2022); *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 4 (D.D.C. Sept. 21, 2022).
[32] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 46, 52 (D.D.C. Sept. 7, 2022).
[33] *Id.* at 54.
[34] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 54 (D.D.C. Sept. 7, 2022); *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 10 (D.D.C. July 22, 2022).

because EDI clearinghouses have agreements to transmit claims they receive from other EDI clearinghouses on behalf of each EDI's clearinghouse.[35]

164. The ubiquity of the Change Platform is largely a function of its vast network of relationships with payers and providers.[36] Indeed, as of March 6, 2024, Change Healthcare had an exclusive payer arrangement with over 1000 payers in the United States, including in several states, Aetna, BlueCross/Blue Shield, Kaiser, and Medicaid.[37] Such payers only accepted electronic claims through the Change Platform. Including exclusive payers, Change's pervasive network connectivity includes a network of approximately 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, 600 laboratories, and 2,400 government and commercial health insurers.[38]

165. At the time of its merger with Optum Insight, Change Healthcare operated the country's largest EDI clearinghouse with over half of all commercial medical claims data flowing through the Change Platform.[39] Using its EDI clearinghouse network, Change Healthcare's Network Solutions business facilitates "'financial, administrative, and clinical transactions, electronic business-to-business and consumer-to-business payments,' as well as aggregation and analytical data services," and generally the transmission of electronic

[35] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 10 (D.D.C. July 22, 2022).
[36] *Id.* at 56.
[37] *Exclusive Change Healthcare Payers for Claims* (Mar. 6, 2024), https://support.drchrono.com/home/23548386475163-exclusive-change-healthcare-payers-for-claims-as-of-3-06-2024 (last visited Nov. 26, 2024).
[38] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Change's Answer to DOJ Complaint, Dkt. No. 38 at 4, 7 (D.D.C. Mar. 11, 2022).
[39] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 8, 34 (D.D.C. Sept. 21, 2022).

claims.[40] Specifically, Change Healthcare processes approximately $1.5 trillion in medical claims annually via 15 billion healthcare transactions, and a third of the patient records in the United States pass through the Change Platform.[41] Indeed, at the time of its merger with Optum Insight, "Change [Healthcare] [brought] to the table over 50 million lives in interoperability and 700 vendor partnerships, in total, touching one in three patient records in the United States and helping to facilitate 2.8 billion clinical transactions…unrelated to Change [Healthcare's] EDI network."[42]

166. As a matter of policy and practice, Change Healthcare stores and maintains historical claims data flowing through its EDI clearinghouse from as far back as 2012.[43]

167. Change Healthcare has "primary" and "secondary" use rights over the data transmitted through its clearinghouse "for purposes beyond providing clearinghouse services" and licenses de-identified data to third parties.[44] In January 2021, Optum

[40] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 46, 52 (D.D.C. Sept. 7, 2022).
[41] *Opening Statement Testimony of Senator Ron Wyden*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf at 1 (last visited Nov. 26, 2024); *Opening Statement Testimony of Senator Mike Crapo*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf at 1 (last visited Nov. 26, 2024).
[42] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 73-74 (D.D.C. Sept. 7, 2022).
[43] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Change's Answer to DOJ Complaint, Dkt. No. 38 at 11 (D.D.C. Mar. 11, 2022).
[44] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 8 (D.D.C. Sept. 21, 2022).

estimated that Change Healthcare had data rights for approximately 90 million Americans.[45]

JURISDICTION AND VENUE

168. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class members who are diverse from Defendant, and (4) there are more than 100 Class members.

169. This Court has personal jurisdiction over each of Defendants because at all relevant times, each Defendant operated its principal places of business in this State and also because each Defendant took actions in this State that gave rise to the Data Breach and, thus, to Plaintiffs' and the Class's claims.

170. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendants UHG, Optum, Inc. and Optum Insight, Inc. are residents of this District, and a substantial part of the events giving rise to Plaintiffs' claims occurred here.

171. Venue is proper in this District for pretrial pursuant to 28 U.S..C § 1407(a) and the Order by the Judicial Panel on Multidistrict Litigation consolidating related actions before this Court.

[45] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 87 (D.D.C. Sept. 7, 2022).

172. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

FACTUAL ALLEGATIONS

I. The Change Platform

A. Change Platform is used throughout the healthcare industry

173. The Change Platform is Change Healthcare's suite of revenue management, clinical, and patient support software.

174. Change Healthcare advertises its Change Platform as providing "industry-leading analytics, expansive data, and unparalleled connection and data transfer between providers, payers, and consumers to help improve workflows, increase administrative and financial efficiencies, and improve clinical decisions."[46]

175. The Change Platform is ubiquitous in the healthcare industry, with a network of "800,000 physicians, 117,000 dentists, 60,000 pharmacies, 5,500 hospitals, nearly 400 vendors and 600 laboratories as well as nearly all government and commercial payers."[47]

176. "Change Healthcare processes 15 billion health care transactions annually and touches 1 in every 3 patient records."[48]

---

[46] *About*, Change Healthcare, https://cs-gw-www.staging.changehealthcare.com/about (last visited Dec. 9, 2024).
[47] Katie Terrell Hanna & Sarah Lewis, *What is Change Healthcare?*, TechTarget, https://www.techtarget.com/searchhealthit/definition/Change-Healthcare (last updated Sept. 2024).
[48] *AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances*, Am. Hosp. Assoc. (Mar. 2024), https://www.aha.org/2024-03-15-

B. The Change Platform collects the Personal Information of millions of individuals

177. The value and usefulness of the Change Platform is predicated on healthcare providers and patients inputting highly sensitive Personal Information into the platform. Those inputs are necessary for the Change Platform to help Defendants and others to whom they sell the data effectuate revenue management, clinical decision making, and patient support.

178. Data that is typically entered into the Change Platform include full names, phone numbers, addresses, Social Security numbers, dates of birth, email addresses, medical records, specific treatment information, dental records, payment information, claims information, and insurance records.

179. Change Healthcare has kept and maintained the information it has collected over years of providing its services, including aggregating and storing information in the legacy server that would ultimately be accessed and exfiltrated by unauthorized users during the Data Breach.

C. Defendants Function as One Entity to Commoditize Personal Information for Monetary Gain

180. Personal health data has never been more ubiquitous or more valuable. The global investment banking firm RBC Capital Markets estimates that 30% of the world's data is now being generated in the healthcare sector and that healthcare data alone will

---

aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances.

grow at a Compound Annual Growth Rate ("CAGR") of 36% by 2025.[49] This development is the result of improved software technologies, increased detail in information collected as part of medical encounters, more sophisticated billing processes, improved data storage, and rapid conversion to EHR. Between 2009 and 2019, U.S. hospital adoption of EHR systems grew from 6.6% to 81.2%. [50]

181. This accumulation of data creates the opportunity for commercial exploitation. Commercial data analytic efforts and techniques have evolved simultaneously to accommodate the volume, velocity and variety of these innumerable individual health records.[51] The global data analytics market was valued at $43.1 billion in 2023 and expected to grow by 23% the next year, reaching $53 billion in 2024.[52] The consulting firm McKinsey estimates healthcare data analytics profits are growing at a CAGR of 22%.[53] One healthcare data firm—IQVIA, a "global provider of advanced analytics, technology solutions, and clinical research services" —reported revenue of $14.9 billion for 2023.

---

[49] *The Claims Processing Manual,* 2019, American Medical Billing Association, https://www.ambastore.net/product_p/advancedclaimsmanual1.htm (last visited Dec. 11, 2024).
[50] *Compare PPOs, EPOs, and HMOs*, California Department of Insurance, https://www.insurance.ca.gov/01-consumers/110-health/10-basics/compare.cfm (last visited Dec. 16, 2024).
[51] *Types of Health Coverage*, California Department of Insurance, https://www.insurance.ca.gov/01-consumers/110-health/10-basics/types.cfm (last visited Dec. 16, 2024).
[52] *Change Healthcare, Form 10-K for fiscal year ending March 31, 2022*, SEC, https://www.sec.gov/Archives/edgar/data/1756497/000175649722000007/chng-20220331x10k.htm.
[53] Henderson, Morgan A., and Morgane C. Mouslim, *Facts About Hospital-Insurer Contracting*, *The American Journal of Managed Care* 30, no. 2 (Feb. 2024).

182. As an example, in 2021, Optum Insight generated approximately $12 billion in revenue and UHC was its largest customer. In 2022, Optum Insight estimated that it handled 22 billion transactions and managed $120 billion in billings for its "revenue cycle clients." To do so, Optum utilized clinical and claims data on approximately 285 million "lives" (*i.e.*, people).

183. The key driver in the growth of healthcare data analytics is the availability of new artificial intelligence (AI) and machine learning. These rapidly advancing techniques make it possible with historical data to build an AI model that can more reliably predict future events and outcomes.

184. The future predictors include prevalence of specific medical conditions, probability of disease progression with differing forms of interventions, costs of future medical claims for specific populations with differing demographic characteristics, cost savings likely to be achieved through shorter hospital stays and avoidance of infection, and countless other outcomes. The key limitation is the quantity and quality of data available with which to "train" the AI model. The simple rule for training the AI model and increasing its accuracy in prediction is "the more data, the better."

185. Cognizant of "the more data, the better," UHG purchased Change Healthcare to acquire its database of patients' individual medical claims via its clearinghouse role. To this end, UHG's acquisition of Change Healthcare and its merger with Optum Insight enabled it to obtain data on over 50% of all medical claims in the United States. Put simply, Optum Insight substantially increased its patient information database through the acquisition of Change Healthcare.

186. Change Healthcare's data analytics tools enabled it to advise insurers on how to improve profitability by narrowing coverage or increasing the applicable health insurance rate.

187. Notably, in its 10-K filing, Change Healthcare identified two primary customer groups for its products: payors and providers. Payors included national commercial insurers, regional private insurers, Blue Cross Blue Shield Plans, Medicare/Medicaid plans, provider-sponsored payors, third-party administrators, and other specialty health benefits insurers. Providers included hospitals and health systems, physician practices, dentists, pharmacies, skilled nursing facilities, home health agencies, telehealth providers, senior care facilities, laboratories, and other healthcare providers. UHG contains both healthcare providers and payors under its umbrella.[54]

188. Change Healthcare maintained an EDI clearinghouse through which claims between providers and payors were submitted, verified, adjusted, and resolved. Those processes required large amounts of Personal Information (*e.g.*, entire medical histories, doctor's notes, lab results, etc.) and third-party insurer's information (*e.g.*, claims rates, reimbursement rates, network members, etc.) to be placed into the EDI clearinghouse of Change Healthcare.

189. At the time of its merger with Change Healthcare in 2022, Optum Insight processed approximately 192 million medical claims annually via its EDI clearinghouse

[54] *Optum Insight Overview*, Optum Insight, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/ic23/UHG_IC23_OI_Overview_Highlights.pdf (last visited Dec. 10, 2024).

on behalf of approximately 220 of the approximately 230 health insurance companies in the United States.[55] Via its own EDI clearinghouse network, Optum Insight had the largest collection of claims and electronic medical records in the healthcare industry, covering approximately 270 million American lives.[56] The claims data "sent to Optum Insight [] is not de-identified or masked in any way."[57]

190. As a Software as a Service (SaaS) company, Change Healthcare generated 46.3% of its 2022 fiscal year revenue through its "Software and Analytics" segment via its fixed fee and per-transaction fee arrangements, content subscriptions licenses, and software licenses. The remainder of its revenue was generated through "Network Solutions" and "Technology-Enabled Services" segments, which include support and consulting services for financial, administrative, clinical and pharmacy transactions, electronic payments and aggregation and analytics of clinical and financial data, claims processing, and training and consulting services.[58]

191. Change Healthcare stated that its software and analytics products sought to "navigate the industry's transition to value-based care" by providing software for revenue cycle management, provider network management, payment accuracy, value-based

[55] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 19-20 (D.D.C. Sept. 7, 2022).
[56] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 12 (D.D.C. July 22, 2022).
[57] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 21, 26 (D.D.C. Sept. 7, 2022).
[58] *Optum Insight Overview*, Optum Insight, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/ic23/UHG_IC23_OI_Overview_Highlights.pdf (last visited Dec. 10, 2024).

payments, clinical decision support, consumer engagement, risk adjustment and quality performance, and imaging and clinical workflow. All of these tools used to transition to value-based care, also known as "pay for performance," require the analysis of large quantities of claims and clinical data.

192. As part of the merger between Change Healthcare and Optum, UHG acquired data on more than 14 billion total transactions, representing over 50% of U.S. medical claims. [59] Change Healthcare had secondary-use rights to over 60% of the claims data that passed through its EDI clearinghouse. A secondary-use right is the right for Change Healthcare to use the data that enters its EDI clearinghouse for Change Healthcare's purposes above and beyond the purpose for which it was initially submitted to the clearinghouse (*e.g.*, insurance claim processing).

193. According to the closing statement in litigation brought by the United States Department of Justice opposing the merger,[60] Mr. Tim Suther, Senior Vice President and General Manager of Data Solutions at Change Healthcare, agreed with the characterization of those secondary-use rights as "unfettered." The end result of the acquisition was that UHG more than doubled the amount of claims data its subsidiaries could use for machine learning, AI predictive modeling, and strategic business endeavors and profit.

194. The new data acquired by Change Healthcare had special, strategic value for UHG and its health insurer UHC because it afforded them with the ability to identify

[59] *IQVIA Reports Fourth-Quarter and Full-Year 2023 Results; Issues Full-Year 2024 Guidance*, IQVIA (Feb. 14, 2024), https://www.iqvia.com/newsroom/2024/02/iqvia-reports-fourth-quarter-and-full-year-2023-results.

[60] *See U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-00481 (D.D.C.).

competing insurer practices in underwriting, claims experience, and provider reimbursements. The data also allowed UHG and UHC to learn about competing provider networks and claims rates for specific conditions and procedures. With the data, UHG supports its Optum business efforts and simultaneously steers UHC away from insuring higher risk populations determined to be a "bad risk."

195. The use of Change Healthcare's data to help UHG and its subsidiaries mirrors UHG's goal of having its subsidiaries act in unison as "one" entity. UHG's Chief Growth Strategy Officer, Daniel Schumacher, discussed having a "one United" approach to business decisions, both within and across affiliates, that would "remove the silos," despite the sensitivity of the shared data.[61] In other words, Mr. Schumacher admitted that UHC, Optum, and Change Healthcare all operate collectively as one to achieve the same goal—increased profits to UHG using patient data.

196. The claims data obtained from Change Healthcare also benefitted Optum Insight in marketing to other insurers and self-funded employer and labor organization-sponsored health plans wanting to refine their own underwriting, benefit structures, provider networks and contract negotiations.[62]

---

[61] *United States of America, State of New York, & State of Minnesota v. UnitedHealth Group Inc. & Change Healthcare Inc., Closing Statement*, U.S. Dep't of Justice, https://www.justice.gov/d9/2024-03/406897.pdf (last visited Dec. 10, 2024).

[62] Raghupathi, Wullianallur, and Viju Raghupathi, *Big data analytics in healthcare: promise and potential*, Health Information Science and Systems 2, no. 3 (Feb. 2014), https://pmc.ncbi.nlm.nih.gov/articles/PMC4341817/; *see also The Healthcare Data Explosion*, RBC Capital Markets, https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion (last visited Dec. 10, 2024).

197. Further, both Change Healthcare and Optum Insight marketed their services to providers to improve their claims success. For example, Optum's "Enterprise CAC and CDI 3D" provides code suggestions for medical claims, powered by "Optum Clinical Language Intelligence." These suggestions promise to "support accurate revenue integrity, higher coding accuracy, and reduced denials." Both Change Healthcare and Optum Insight also claimed to provide valuable advice for providers on the most cost-effective treatments. This type of guidance is typically developed from extensive patient data regarding actual outcomes and costs. [63]

198. For instance, in promoting its "Optum® Performance Analytics: A unified health care data and analytics platform," Optum explains how "clinical and claims data assets with a growing set of social demographics, behavioral, patient-reported and quality outcome data can give you a more comprehensive view of each patient, provider, and facility, as well as an aggregated understanding of your entire population and health network." Optum represents that its analysis can provide "complete retrospective views" on patients and networks, tracking utilization, referral patterns, cost, and physician performance and that its analytics products can help monitor the quality and cost of physician networks. Optum makes this representation because of its enhanced data analytics based on the data it possesses, including that obtained from Change Healthcare; this data represents the Personal Information of Plaintiffs and Class members. [64]

[63] Raghupathi, et al., *supra* note 62.
[64] *Id*.

199. By way of another example, Change Healthcare's data also informed UHG and Optum about how UHC's rival health insurers control utilization, such as competing insurer's cost-sharing tools, service limitations, and prior authorization policies. Using Optum Insight's analytics software, hospitals, and other healthcare organizations were told they could achieve reductions in the least profitable medical services.[65]

200. In simple terms, UHG's acquisition of Change Healthcare via Optum Insight advanced its already ongoing data analytics through analysis of patient information on Change Healthcare's own database—*i.e.*, Plaintiffs' and Class members' Personal Information. UHG purchased Change Healthcare because its data benefited it and each of its subsidiaries collectively.

D. Prior to the Data Breach, UHG Defendants warranted the security of the Change Platform and its safeguard of patient Personal Information

201. UHG, Optum, and UHC all operate and operated prior to the Data Breach under the same privacy policy. They represent that they maintain "administrative, technical, and physical safeguards" designed to protect patients' information.[66]

202. Given their current and prior representations and wide range business practices of handling highly sensitive Personal Information, UHG, Optum, Optum Insight, and Change Healthcare understood the need to protect patients' privacy and prioritize data security.

---

[65] *Id*.

[66] *See*, *e.g.*, *Online Services Privacy Policy*, UnitedHealth Group, https://www.unitedhealthgroup.com/privacy.html (last visited Dec. 3, 2024).

203. Change Healthcare's Global Privacy Notice represented that "Privacy matters to Change Healthcare, so we follow a privacy framework that helps us to manage and protect your personal information…."[67] Change Healthcare further represented that they implemented and maintained "security measures designed to safeguard the data we process against unauthorized access..." such that "Your personal information is only accessible to personnel who need to access it…."[68]

204. Likewise, Change Healthcare represented in its Code of Conduct[69] that:

a. "We exercise care and discretion when handling [restricted and confidential] information."

b. "We collect, store, access, use, share, transfer, and dispose of [personally identifiable information] responsibly."

c. "We also respect and protect the sensitive nature of [protected health information] and carefully maintain its confidentiality."

d. "We earn the trust of our team members and the companies with which we do business by following our privacy, security, and data and information protection policies."

[67] *Global Privacy Notice*, Change Healthcare, https://www.changehealthcare.com/privacy-notice.html (last visited Dec. 18, 2024).
[68] *Id.* The Notice also defines "your" as used here to include the patients and consumers of the entity payer and provider customers for which it is a HIPAA business associate.
[69] *Our Code of Conduct*, Change Healthcare, https://codeofconduct.changehealthcare.com/ (last visited Dec. 19, 2024).

e. "We also regularly monitor our systems to be sure that information is accessed and used for appropriate, authorized activities, to discover any new threats, and to look for ways to improve."

f. "We monitor and control all electronic and computing devices used … to interact with our internal networks and systems."

205. Hence, prior to the Data Breach, Change Healthcare recognized and acknowledged that its customers and those it services have placed their trust in Change Healthcare to protect the confidentiality and privacy of their data and "the consequences of betraying the trust of its customers…would be catastrophic."[70] Change Healthcare is abd was responsible to all those who place their trust in it to maintain data security, including the patients and consumers who are ultimately served by its platform and services, such as Plaintiffs and Class members.

206. Defendants represented to the public that these are not mere words or policies. Optum Insight's Chief Operating Officer has testified that the company's culture is to "treat customers' data as they would treat their data themselves."[71] Defendants represented, under oath, that they had built a top down "culture of trust and integrity around protecting customers' sensitive information."[72]

[70] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 66 (D.D.C. Sept. 7, 2022).
[71] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 40 (D.D.C. Sept. 21, 2022).
[72] *U.S. v. UnitedHealth Group, Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 30 (D.D.C. Sept. 7, 2022).

207. Change Healthcare also held out that it has various processes and policies in place to protect their clients' and patients' sensitive information: "Keeping our customers' information secure is a top priority for Change Healthcare. We dedicate extensive resources to make sure personal medical and financial information is secure and we strive to build a company culture that reinforces trust at every opportunity."[73]

208. Accordingly, as stated on its website, Change Healthcare assured the following:

> We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information. We evaluate and update these measures on an ongoing basis. Your Personal Information is only accessible to personnel who need to access it to perform their duties.[74]

209. As part of the merger with Change Healthcare, UHG made "binding commitments" to customers to apply and maintain data security policies to protect customers' data "and to uphold all contractual rights of Change Healthcare's customers to audit the protection and security of their data."[75]

210. Given the extensive amount and sensitive nature of the data they handle, Defendants maintain privacy policies outlining the usage and disclosure of confidential and personal information. UHG and Optum adhere to the same "Privacy Policy," which assured

---

[73] *Accreditations & Certifications*, Change Healthcare, https://www.changehealthcare.com/accreditations-certifications (last visited July 16, 2024).
[74] *Privacy at Change Healthcare*, Change Healthcare, https://www.changehealthcare.com/privacy-notice (last visited Mar. 11, 2024).
[75] *Id.* at 107-08.

and currently assures the public that Defendants have implemented "administrative, technical, and physical safeguards" to safeguard patients' information. Their "Social Security Number Protection Policy" explicitly stated their commitment to preserving the confidentiality of Social Security numbers received or collected during business operations. Defendants also pledged to limit access to Social Security numbers to lawful purposes and to prohibit unlawful disclosure.[76]

211. Given their prior and current representations and experience handling highly sensitive PII and PHI, Defendants understood the need and requirements to protect patients' Personal Information and prioritize data security.

E. Change Healthcare's outdated and unsecure cybersecurity protocols left it vulnerable to a data breach

1. Change Healthcare's networks can be remotely accessed without multi-factor authentication through a phishing scheme.

212. Change Healthcare employees were able to access Change Healthcare's internal networks remotely through third-party Citrix Remote PC Access software.[77]

213. Citrix's "Remote PC Access is a feature of Citrix Virtual Apps and Desktops that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by

[76] *Online Services Privacy Policy*, UnitedHealth Group, https://www.unitedhealthgroup.com/privacy.html (last visited Dec. 3, 2024).
[77] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work."[78]

214. Change Healthcare's implementation of Citrix Remote PC Access was not equipped with multi-factor authentication ("MFA"), "an identity verification method in which a user must supply at least 2 pieces of evidence, such as their password and a temporary passcode, to prove their identity."[79] "For example, to log into an email account, a user might need to enter both their account password and a single-use passcode the email provider sends to their mobile phone via text message."[80]

215. "MFA systems add an extra layer of security by requiring more than one piece of evidence to confirm a user's identity. Even if hackers steal a password, it won't be enough to gain unauthorized access to a system."[81]

216. "MFA has become an increasingly important piece of corporate identity and access management (IAM) strategies. Standard single-factor authentication methods, which rely on usernames and passwords, are easy to break. In fact, compromised credentials are one of the most common causes of data breaches, according to IBM's *Cost of a Data Breach* report."[82]

---

[78] *Remote PC Access*, Citrix (Sept. 6, 2024), https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure/remote-pc-access.html.
[79] Matthew Kosinski & Amber Forrest, *What is MFA?*, IBM (Jan. 4, 2024), https://www.ibm.com/topics/multi-factor-authentication.
[80] *Id.*
[81] *Id.*
[82] *Id.*

217. According to the Federal Bureau of Investigation ("FBI"), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[83]

218. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[84]

219. Through technological security barriers, companies can greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework ("SPF") (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail ("DKIM") (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance ("DMARC"), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding

[83] *Internet Criminal Report 2020*, FBI (2020), https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf.
[84] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, CISA (Oct. 29, 2020), https://www.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.

a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[85]

220. In 2019, both Microsoft and Google publicly reported that using MFA blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating: "[t]ime to implement multi-factor authentication!"[86]

221. The FBI concurs, listing "applying two-factor authentication wherever possible" as a best practice to defend against ransomware attacks.[87]

222. Citrix states on their website that "it is crucial . . . to also implement multi-factor authentication as a backup in case passwords do become compromised."[88]

223. Change Healthcare's internal networks are accessible through Citrix Remote PC Access without MFA, meaning that any third party that obtained a Change Healthcare employee's login credentials could access Change Healthcare's internal networks remotely.

---

[85] *Id.*
[86] Matt Bromiley, *Bye Bye Passwords: New Ways to Authenticate*, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.
[87] *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), https://www.ic3.gov/PSA/2016/psa160915.
[88] *What is a single sign-on*, Citrix, https://www.citrix.com/glossary/what-is-single-sign-on-sso.html (last visited Dec. 3, 2024).

2. Lack of internal cybersecurity monitoring

224. Change Healthcare, while acting as a clearinghouse for millions of individuals' most sensitive Personal Information, did not have adequate cybersecurity monitoring systems in place to prevent unauthorized access to its networks.

225. A key component of cybersecurity monitoring is an intrusion detection system, which "analyzes an organization's network traffic, activities, and devices, looking for known malicious activities or policy violations. If an IDS detects suspicious activities or patterns, it alerts the system administrators or security team of the potential threat."[89]

226. "Cybersecurity or process monitoring also involves continuously observing and analyzing your computer network or systems to prevent cyberattacks. The primary objective of monitoring in cybersecurity is quickly identifying signs of vulnerability and responding to potential security threats in real-time."[90]

227. Change Healthcare's systems lacked internal monitoring to such a degree that the attackers were not detected until they chose to reveal themselves—9 days after gaining access.

228. ALPHV's activity involved several steps that should have been noticed by Change Health Defendants through proper endpoint and network monitoring and scanning. This includes:

---

[89] *Cyber Security Monitoring: Definition and Best Practices*, SentinelOne (Oct. 16, 2024), https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/.

[90] *Cyber Security Monitoring: Definition and Best Practices*, SentinelOne (Oct. 16, 2024), https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/.

a. Installing software such as nmap. Nmap is an obvious and 'noisy' network discovery scanner.[91] Only administrators should be able to install any software, and then such installations should still be monitored.[92] Had Change Healthcare properly monitored its systems, it would not have allowed nmap to be installed in the first instance. A properly monitored network would have also detected nmap being installed. Application whitelisting, which means even administrators can only install software that has been pre-approved[93] would have also prevented the installation of nmap because nmap would not have been on the whitelist.

b. The attackers also ran several administrator-only commands. These commands should only be possible for those with the highest of security privileges, and even then, the execution of these privileges

[91] Daryna Olyniychuk, *Detect ALPHA SPIDER Ransomware Attacks: TTPs Leveraged by ALPHV aka BlackCat RaaS Operators*, SOC Prime (Mar. 15, 2024), https://socprime.com/blog/detect-alpha-spider-ransomware-attacks-analysing-ttps-leveraged-by-alphv-BlackCat-raas-operators/.

[92] *Limit Software Installation*, Mitre Att&ck, https://attack.mitre.org/mitigations/M1033/ (last updated Oct. 17, 2024); *Restrict Software on Windows Devices Using a Policy*, Jumpcloud, https://jumpcloud.com/support/restrict-software-on-windows-devices-using-policy (last visited Jan. 2, 2025); *What Is a Software Restriction Policy?*, Heimdal, https://heimdalsecurity.com/blog/software-restriction-policy/ (last updated Dec. 8, 2023).

[93] *Protecting Against Malicious Code*, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security, https://www.cisa.gov/news-events/news/protecting-against-malicious-code (last updated Nov. 19, 2019); Katie C. Stewart, *Establish and Maintain Whitelists*, Software Engineering Institute, Carnegie Mellon University (Oct. 25, 2017), https://insights.sei.cmu.edu/blog/establish-and-maintain-whitelists-part-5-of-7-mitigating-risks-of-unsupported-operating-systems/.

should be logged and monitored. Had Change Healthcare had proper monitoring on its networks, the administrator-only commands would have alerted Change Healthcare's IT personnel.

c. The attackers exfiltrated terabytes of Personal Information. Such actions should have only been possible by Change Healthcare network administrators and should have required even administrators to pass additional security features. Such exfiltration activity should have been detected and raised numerous red flags to Change Healthcare had it properly monitored its system.

229. Had Change Healthcare implemented adequate internal cybersecurity monitoring, the Data Breach and shutdown would have been prevented or much smaller in scope.

230. "One of the simplest yet effective methods of safeguarding systems is through IP whitelisting. It is particularly beneficial for businesses that rely on remote access or have distributed teams but want to maintain strict security protocols. . . . IP whitelisting is a security practice that involves creating a list of trusted IP addresses granted access to a specific server, application, or network. By using IP whitelisting, only pre-approved IP addresses can interact with your system. By restricting access to a select group of devices based on their IP addresses, you can limit exposure to potential attacks

and unauthorized access. The method effectively controls access to critical business systems, cloud infrastructure, and online services."[94]

231. The United States Dept. of Commerce has also produced guidance for application whitelisting, NIST Special Publication 800-167: *Guide to Application Whitelisting,* which provides specific guidance to companies on how to implement whitelisting, to prevent "installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software."[95]

II. The Data Breach

A. ALPHV cybercriminal ransomware group

232. ALPHV is a Russian-speaking cybercriminal ransomware group that emerged in 2021. ALPHV is also commonly known as BlackCat due to the image of a black cat on its ransomware dark web site.[96]

233. "ALPHV operates as a Ransomware-as-a-Service (RaaS), which means fellow threat actors can become affiliates by purchasing access to ALPHV ransomware, infrastructure, and other resources. ALPHV affiliates conduct attacks, while ALPHV focuses on affiliate support, ransomware development, and business expansion."[97]

---

[94] Timothy Shim, *IP Whitelisting: The Beginner's Guide*, Rapid Seedbox, (Oct. 7, 2024), https://www.rapidseedbox.com/blog/ip-whitelisting.
[95] *NIST Special Publication 800-167, Guide to Application Whitelisting*, NIST (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.
[96] Christine Barry, *ALPHV-BlackCat ransomware group goes dark*, Barracuda (Mar. 7, 2024), https://blog.barracuda.com/2024/03/06/alphv-blackcat-ransomware-goes-dark.
[97] *Id.*

234. ALPHV is notably sophisticated in its use of the Rust programming language, "which improve[s] attack performance."[98]

235. ALPHV cybersecurity attacks often use the "double extortion" method, whereby a victim's data is both ransomed—*i.e.*, stolen with the threat of publication if a ransom is not paid—and encrypted—*i.e.*, turned into an unreadable format on the victim's network, so that the victim cannot continue using the data without ALPHV's decryption key.[99]

236. ALPHV also sometimes use "triple extortion" which additionally adds the threat of a distributed denial of service (DDoS) attack, which can shut down a victim's networks.[100]

237. ALPHV has collected nearly $300 million in ransom as of 2023 and already gained notoriety for high-profile attacks targeting healthcare entities.[101]

238. "FBI identified ALPHV/Blackcat actors as having compromised over 1,000 victim entities in the United States and elsewhere, including prominent government entities (*e.g.*, municipal governments, defense contractors, and critical infrastructure organizations)."[102]

---

[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Reward for Information: ALPHV/Blackcat Ransomware as a Service*, U.S. Dep't of State (Feb. 15, 2024), https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/.

239. The U.S. Department of Health and Human Services has recognized ALPHV ransomware as a sophisticated threat to the health sector since at least 2023.[103]

240. "The U.S. Department of State is offering a reward of up to $10,000,000 for information leading to the identification or location of any individual(s) who hold a key leadership position in the Transnational Organized Crime group behind the ALPHV/Blackcat ransomware variant."[104] In January of 2023, Nextgen Health, "a multibillion-dollar healthcare giant [that] produces electronic health record (EHR) software and practice management systems for hundreds of the biggest hospitals and clinics in the U.S.," was attacked by ALPHV Blackcat ransomware.[105]

241. In February of 2023, ALPHV Blackcat successfully penetrated the Lehigh Valley Health Network systems and exfiltrated and published sensitive patient data including clinical images of breast cancer patients that the group notoriously teased as "nude photos."[106]

---

[103] *Royal & BlackCat Ransomware: The Threat to the Health Sector*, U.S. Dep't of Health and Human Servs. (Jan. 12, 2023), https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

[104] *Reward for Information: ALPHV/Blackcat Ransomware as a Service*, U.S. Dep't of State (Feb. 15, 2024), https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/.

[105] Jonathan Greig *Electronic health record giant NextGen dealing with cyberattack* (Jan. 19, 2023), https://therecord.media/electronic-health-record-giant-nextgen-dealing-with-cyberattack.

[106] Alexander Martin *Ransomware gang posts breast cancer patients' clinical photographs* (Mar. 6, 2023), https://therecord.media/ransomware-lehigh-valley-alphv-black-cat.

242. In July 2023, ALPHV Blackcat attacked Barts Health NHS Trust in the UK and exfiltrated seven terabytes of information.[107]

243. In October of 2023, ALPHV Blackcat took credit for a July 2023 attack on McLaren Health Care, where they successfully exfiltrated the PII and PHI of over 2.2 million McLaren patients.[108]

244. According to John Riggi, the AHA's national advisor for cybersecurity and risk, as of December 20, 2023 "[ALPHV Blackcat] has attacked numerous hospitals, publicly exposed sensitive patient data and placed patient care and lives at risk."[109]

245. On December 19, 2023 the FBI and the Cybersecurity and Infrastructure Security Agency ("CISA") co-authored another Joint Cybersecurity Advisory titled "#StopRansomware: ALPHV Blackcat" warning that ALPHV Blackcat was targeting critical infrastructure with ransomware and identified certain Indicators of Compromise ("IOCs") associated with the ransomware group.[110] The warning specifically noted that "[s]ince previous reporting, ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide [nearly 75 percent of which are in the United States] targeted via ransomware and/or data extortion."

---

[107] *BlackCat/ALPHV Ransomware: In-Depth Analysis And Mitigation* https://stonefly.com/blog/blackcat-alphv-ransomware-analysis-and-mitigation/.

[108] Bill Toulas *McLaren Health Care says data breach impacted 2.2 million people* (Nov. 10, 2023) https://www.bleepingcomputer.com/news/security/mclaren-health-care-says-data-breach-impacted-22-million-people/.

[109] *DOJ disrupts ALPHV/Blackcat ransomware group: AHA News* (Dec. 20, 2023) https://www.aha.org/news/headline/2023-12-20-doj-disrupts-alphvblackcat-ransomware-group.

[110] *Joint Cybersecurity Advisory- #StopRansomware: ALPHV Blackcat* (Dec. 19, 2023) https://www.aha.org/system/files/media/file/2023/12/joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf.

246. The report further warned that "ALPHV Blackcat affiliates use advanced social engineering techniques and open-source research on a company to gain initial access. Actors pose as company IT and/or helpdesk staff and use phone calls or SMS messages to obtain credentials from employees to access the target network. ALPHV Blackcat affiliates use uniform resource locators (URLs) to live-chat with victims to convey demands and initiate processes to restore the victims' encrypted files."

247. The advisory further recommended that potential targets implement certain precautions to "to improve your organization's cybersecurity posture based on threat actor activity and to reduce the risk of compromise by ALPHV Blackcat threat actors."

248. As far back as 2022, and continuing to 2023, independent security researchers also published guides detailing ALPHV Blackcats' attacks vectors, known IOCs, and prophylactic measures organizations could implement to detect, prevent, or mitigate the group's ransomware attacks.[111]

249. As described, the steps of an ALPHV attack are well-documented, as are the defenses that can be employed at each step to foil an attack. An overview of a standard process is given here[112]:

---

[111] *BlackCat/ALPHV Ransomware: In-Depth Analysis and Mitigation*, StoneFly https://stonefly.com/blog/blackcat-alphv-ransomware-analysis-and-mitigation/ (last visited Jan. 14, 2025); Amanda Tanner, *Threat Assessment: BlackCat Ransomware*, Unit 42 (Jan. 27, 2022), https://unit42.paloaltonetworks.com/blackcat-ransomware/.

[112] *A Deep Dive Into ALPHV/BlackCat Ransomware*, SecurityScorecard, https://securityscorecard.com/research/deep-dive-into-alphv-BlackCat-ransomware (last visited Jan. 2, 2025); *What is BlackCat Ransomware*, Akamai, https://www.akamai.com/glossary/what-is-BlackCat-ransomware (last visited Jan. 2, 2025); Mehardeep Singh Sawhney, *Technical Analysis of ALPHV/BlackCat*

a. Initial access often begins with obtaining login credentials and exploiting systems that do not have MFA.

b. After access is achieved, the network is scanned for other machines. A network scan, particularly using such a widely known tool as NMAP, should be detected by any properly configured system monitoring.

c. They next use a tool named PsExec[113] to deploy additional malware to other systems on the network. This tool is a free tool but must be downloaded and installed on the machine. If the victim systems are using the very fundamental cybersecurity principle of least privileges, then only a select few accounts would even be able to install software. This would mean that if the attackers gained access through an account that was not part of the group that had privileges to install software, their attack would be stopped.

d. The tool the attackers deploy is ExMatter.[114] It is a tool written in .Net specifically to exfiltrate data. Specifically, ExMatter will steal user

Ransomware, CloudSek (May 22, 2023), https://www.cloudsek.com/blog/technical-analysis-of-alphv-BlackCat-ransomware; *BlackCat/ALPHV Ransomware: In-Depth Analysis and Mitigation*, Stonefly, https://stonefly.com/blog/BlackCat-alphv-ransomware-analysis-and-mitigation/ (last visited Jan. 2, 2025); Jason Hill, *BlackCat Ransomware (ALPHV)*, Varonis, https://www.varonis.com/blog/blackcat-ransomware (last updated Apr. 14, 2023).

[113] Mark Russinovich, *PsExec v2.43*, Microsoft Learn, Systerinals (Apr. 11, 2023), https://learn.microsoft.com/en-us/sysinternals/downloads/psexec.

[114] *ExMatter*, Malpedia, https://malpedia.caad.fkie.fraunhofer.de/details/win.exmatter (last visited Jan. 2, 2025).

files, compressed files, and databases, then upload them to a Secure File Transfer Protocol server (SFTP)[115]. Properly managed systems should notice any system initiating an SFTP transfer to outside the network.

e. ALPHV will also run a number of commands, all of which should require administrative privileges in a properly configured network:

i. Get device UUID

ii. Stop IIS service

iii. Clean Shadow Copies

iv. List Windows Event logs and try to clear them (this in particular should trigger some monitoring system).

f. Only then does ALPHV encrypt the files.

250. In light of all of the above, Defendants were aware or should have been aware of their obligation to implement and use reasonable measures to protect the Personal Information of patients, including against actors like ALPHV, and their failure to implement such measures.

B. ALPHV and its affiliates exploited Change Healthcare's security vulnerabilities to steal PII and PHI of millions of individuals

251. On February 12, 2024, ALPHV and its affiliates "used compromised [password] credentials to remotely access a Change Healthcare Citrix [Remote PC Access]

[115] *Analyzing Exmatter: A Ransomware Data Exfiltration Tool*, Kroll (Mar. 22, 2022), https://www.kroll.com/en/insights/publications/cyber/analyzing-exmatter-ransomware-data-exfiltration-tool.

portal, an application used to enable remote access to laptops."[116] The username and password for a low-level, customer support employee's access to Change's Citrix portal were posted in a Telegram group chat that advertises the sale of stolen credentials. The account was a basic, user-level account: it only had access to specific applications and did not have administrator access or credentials.

252. Change Healthcare provided no details on how the cybercriminals obtained the remote credentials.[117]

253. Since Citrix Remote PC Access portal did not have multi-factor authentication, ALPHV experienced very limited roadblocks in gaining access to Change Healthcare's networks with the compromised credentials.[118]

254. Once the criminals gained access to Change Healthcare's networks, they "moved laterally within the systems in more sophisticated ways and exfiltrated data."[119] Specifically, ALPHV created privileged accounts with administrator capabilities that

---

[116] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

[117] Kyle Alspach, *United Health: Compromised Citrix Credentials Behind Change Healthcare Hack*, CRN (Apr. 30, 2024), https://www.crn.com/news/security/2024/unitedhealth-compromised-citrix-credentials-behind-change-healthcare-hack.

[118] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

[119] *Id.*

permitted access to and deletion of any administrator-level activities. These actions went to the heart of Change Healthcare's most critical IT infrastructure but still went undetected by Defendants.

255. ALPHV navigated through Change Healthcare's systems and servers at will, installing multiple malware tools and applications, as well as a number of "backdoors" that would allow the hacker to return to those environments in the event Change Healthcare did detect the suspicious activity and try to block access.

256. This access to systems critical to Change Healthcare's operations by a user-level account went undetected by Defendants for nine days until ALPHV revealed itself when it began to encrypt Change Healthcare's systems on February 21.

257. On that date, ALPHV ransomware was deployed on Change Healthcare's networks, "encrypting Change Healthcare's systems so" they could not be accessed without ALPHV's cooperation.[120]

258. On that same day, in a SEC filing, Defendants announced that "a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems."[121] After detecting the breach, Defendants claimed to have "proactively isolated the impacted systems from other connecting

[120] *Id.*
[121] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.

systems . . . ."[122] Defendants also said they were "working with law enforcement" and allegedly "notified customers, clients and certain government agencies" of the Breach.[123]

259. UHG disclosed that the "network interruption [was] specific to Change Healthcare . . . ."[124] UHG explained they were working to restore Change Healthcare's information technology systems and resume normal operations as soon as possible but informed the SEC that they could not estimate the duration or extent of the disruption at that time.[125]

260. ALPHV has disclosed that the data exfiltrated in the Data Breach includes millions of: "active US military/navy personnel PII," "medical records," "dental records," "payments information," "Claims information," "Patients PII including Phone numbers/addresses/SSN/emails/etc…," "3000+ source code files for Change Health solutions…," "Insurance records," and "many many more." ALPHV warned Defendants that they were "walking on a very thin line be careful you just might fall over."[126]

261. At the May 1, 2024, U.S. House Subcommittee on Oversight and Investigation Hearing, UHG CEO Andrew Witty estimated that one-third of Americans were impacted by the Data Breach.[127] He also admitted that ALPHV gained access to

---

[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] AJ Vicens, *Notorious ransomware group claims responsibility for attacks roiling US pharmacies*, CyberScoop (Feb. 28, 2024), https://cyberscoop.com/ransomware-alphv-healthcare-pharmacies/.
[127] Ashley Capoot, *UnitedHealth CEO estimates one-third of Americans could be impacted by Change Healthcare cyberattack*, CNBC (May 20, 2024),

Defendants' network because of a lack of MFA on a Change Healthcare server. More specifically, ALPHV used compromised credentials to infiltrate Defendants' network through the externally facing Change Healthcare server.[128]

C. UHG's Statements Regarding the Data Breach

262. Following the data breach, UHG continued to issue a series of notifications to its shareholders and the SEC concerning the Data Breach, the operational status of Change Healthcare's information technology systems, and certain positive financial impacts for the Company resulting from the Data Breach.

263. At the very time Plaintiffs and the Class were being harmed from Defendants' actions and inactions, Defendants were actively reaping additional profits. During the system shutdown due to the ransomware, UHG did not experience a dip in income because people like Plaintiffs and Class members were still paying premiums. However, UHG was not paying providers for the medical services its members received because providers were unable to submit claims. UHG held those millions (if not billions) of dollars that should have been paid out for expenses incurred by Plaintiffs and Class members in their cash reserves, earning interest at a time when interest rates were at historic highs.

---

https://www.cnbc.com/2024/05/01/unitedhealth-ceo-one-third-of-americans-could-be-impacted-by-change-healthcare-cyberattack.html.

[128] *Id.*

264. Amidst all the harm Change Health Defendants' conduct inflicted upon the healthcare system and Providers specifically, UHG acknowledged that it experienced certain positive financial impacts resulting from the Ransomware Attack.

265. For example, on April 16, 2024, UHG reported that the business disruptions caused by the Ransomware Attack had a positive $48 million tax effect, with an estimated benefit of $70 to $90 million in year-end impact. UHG estimated the total tax effect of the Ransomware Attack was $189 million for the first quarter with a $305 million to $375 million total tax effect by year end.

266. On July 16, 2024, UHG reported that the total estimated tax effect of the Ransomware Attack was $252 million for the second quarter with an estimated $515 million to $560 million total tax effect by year end. UHG estimated the total tax effect of the direct response as a result of the Data Breach was $182 million for the second quarter and $323 million for the first two quarters combined.

267. These positive tax benefits comport with UHG's representations to the SEC that "the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition…."

268. Even though it was Defendants' lack of data security that placed Plaintiffs' and Class members' Personal Information in the hands of criminals, Defendants were not the party that suffered the harms from these decisions. UHG represented to the SEC that

"the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition…."[129]

269. On April 22, 2024, UHG issued a press release highlighting the nature and scope of the data exfiltrated from Change Healthcare's systems as a result of the Data Breach. Specifically, Witty reported that files containing PHI and PII for a substantial proportion of America's population were among the files exfiltrated.[130] Witty further reported that it would take several months of continued analysis before UHG believed it had enough information to begin notifying impacted customers and individuals.[131]

270. On May 1, 2024, Witty testified before both the House Energy and Commerce Committee and the Senate Finance Committee concerning the Data Breach. Witty confirmed UHG's understanding that "Cyberattacks continue to increase in frequency and significance..." and explained that UHG understood the pervasiveness of these attacks, given UHG's own experiences with over 450,000 intrusion attempts annually, or "a cybersecurity attempted attack every 70 seconds."[132]

271. Witty claimed that since Change Healthcare recently became part of the UHG, they "were in the process of upgrading and modernizing their technology" when the

[129] *UnitedHealth Group Inc. Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[130] *UnitedHealth Group Update on Change Healthcare Cyberattack*, UnitedHealth Group (Apr. 22, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.
[131] *Id.*
[132] *Id.* at 2.

attack happened and that "the attack itself had the effect of locking up the various backup systems which had been developed inside Change before it was acquired."[133]

272. Witty detailed the events of the Data Breach, which he explained began on February 12, 2024, when "compromised credentials [were used] to remotely access a Change Healthcare Citrix portal" via a desktop computer that "did not have multi-factor authentication."[134]

273. Defendants' failure to implement MFA was an explicit violation of UHG's and Change Healthcare's own policies requiring MFA on all external-facing applications.[135]

274. Witty confirmed that ALPHV/BlackCat first "exfiltrated data" that included PHI and PII "cover[ing] a substantial proportion of people in America," between February 17 and 20, 2024, and then, on February 21, 2024, "deployed a ransomware attack inside Change Healthcare's information technology environments, encrypting Change's systems

[133] *House Energy and Commerce Committee, Oversight Subcommittee hearing Examining the Change Healthcare Cyberattack*, Bloomberg Government (May 2, 2024).
[134] *Id.* at 3.
[135] *Witty Response to Questions for the Record*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf at 1.

so [UHG] could not access them."[136] Witty explained that UHG responded by "immediately sever[ing] connectivity with Change's data centers…."[137]

275. The number of individuals in the United States affected by the data breach is astounding. On October 22, 2024, Change Healthcare notified OCR that it had already sent individual notices to approximately 100 million Americans affected.[138]

D. ALPHV successfully exploited a ransom payment from UHG Defendants without destroying the stolen data

1. ALPHV exploited a ransom demand from UHG Defendants

276. Witty confirmed that PHI and PII from the exfiltrated files had been posted for approximately a week on the dark web before UHG paid the demanded $22 million ransom in Bitcoin.[139,140]

---

[136] *Opening Statement Testimony of UHG CEO Andrew Witty*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf at 2-3; and *Witty Response to Questions for the Record*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf at 9.

[137] *Id.* at 2.

[138] *OCR Change Healthcare Cybersecurity Incident Frequently Asked Questions*, U.S Dept. of Health and Human Services (Oct. 24, 2024), https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html.

[139] *Witty Response to Questions for the Record*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf at 5, 40.

[140] Ashley Capoot, *UnitedHealth CEO tells lawmakers the company paid hackers a $22 million ransom*, CNBC (May 1, 2024), https://www.cnbc.com/2024/05/01/unitedhealth-ceo-says-company-paid-hackers-22-million-ransom.html.

277. Witty made the decision to pay the ransom in exchange for the decryption of Change Healthcare's data.[141]

278. Even though Witty paid the ransom, he could not guarantee that ALPHV and its affiliates did not retain copies of the stolen data.[142]

2. ALPHV received and accepted UHG Defendants' ransom payment without destroying the stolen data

279. After ALPHV received UHG Defendants' ransom payment, it chose not to share the ransom with its affiliate who executed the attack, known as "notchy," and instead, "published a fake law enforcement takedown notice on their leak site before disappearing with the full $22 million."[143]

280. Notchy confirmed that, because it was not paid their share of the ransom by ALPHV, it would retain the stolen data, stating: "Sadly for Change Healthcare, their data [is] still with us."[144]

---

[141] *Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"*, UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf.

[142] *What We Learned: Change Healthcare Cyber Attack*, Energy & Commerce Committee (May 3, 2024), https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

[143] *RansomHub Has Change Healthcare Data – BlackCat/ALPHV Rebrand?*, Halcyon (Apr. 15, 2024), https://www.halcyon.ai/attacks-news/ransomhub-has-change-healthcare-data---blackcat-alphv-rebrand.

[144] *BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare*, Krebs on Security (Mar. 5, 2024), https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/.

281. Notchy and other former ALPHV affiliate groups have since joined the ransomware group RansomHub.[145]

282. RansomHub confirmed that it has reviewed and possesses four terabytes of data stolen from Change Healthcare by posting screenshots on its dark web ransomware site; it has also attempted to extort Defendants out of additional ransom payments.[146]

283. In response to ALPHV refusing to pay Notchy, Dmitry Smilyanets, a researcher for the security firm Recorded Future, said, "[t]he affiliates still have this data, and they're mad they didn't receive this money. . . . It's a good lesson for everyone. You cannot trust criminals; their word is worth nothing."[147]

3. Cybercriminals' promises to destroy stolen data cannot be trusted

284. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks do not just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[148]

---

[145] Christine Barry, *Change Healthcare and RansomHub redefine double extortion*, Barracuda (Apr. 12, 2024), https://blog.barracuda.com/2024/04/12/change-healthcare-and-ransomhub-redefine-double-extortion.

[146] Ionut Arghire, *Ransomware Group Starts Leaking Data Allegedly Stolen From Change Healthcare*, Security Week (Apr. 16, 2024), https://www.securityweek.com/ransomware-group-starts-leaking-data-allegedly-stolen-from-change-healthcare/.

[147] *BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare*, Krebs on Security (Mar. 5, 2024), https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/.

[148] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends.

285. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[149] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[150] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[151] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[152]

286. "The FBI does not support the payment of a ransom in response to a ransomware attack. Paying ransom demands encourages more ransomware incidents and provides an incentive to become involved in this type of illegal activity."[153]

287. Even in cases where compromised companies pay ransom demands, there is no guarantee that the cybercriminals will honor their promise to destroy the stolen data.[154]

---

[149] *The chance of data being stolen in a ransomware attack is greater than one in ten*, https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.
[150] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.
[151] *Id.*
[152] *Id.*
[153] *Reward for Information: ALPHV/Blackcat Ransomware as a Service*, U.S. Dep't of State (Feb. 15, 2024), https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/.
[154] Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, ConsumerAffairs (Nov. 5, 2020), https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html [https://perma.cc/DMV2-JRFP].

288. Indeed, data breach targets that pay ransom demands often cannot substantiate any claimed destruction or return of the data in question.[155]

289. Several media outlets and industry groups have likewise questioned reliance on promises made by cybercriminals.[156]

290. "[N]egotiating for the suppression of stolen data has no finite end. . . . With stolen data, a threat actor can return for a second payment at any point in the future."[157]

E. RansomHub uploaded and offered for sale the stolen data on the dark web

291. On April 16, 2024, RansomHub posted the following on their dark web site, offering for sale four terabytes of stolen Change Healthcare Platform data and confirming

[155] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.") [https://perma.cc/NC7W-T9LJ]; *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html [https://perma.cc/E6K9-HVZZ].

[156] *See, e.g.*, Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/ [https://perma.cc/2LYC-XDP6]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TechCrunch (Oct. 7, 2020), https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/ [https://perma.cc/R8M4-FMMC].

[157] *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, Coveware (Nov. 4, 2020), https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

it not only possessed the information, but had also reviewed the contents of the exfiltrated data..[158]

Change HealthCare - OPTUM Group - United HealthCare Group - FOR SALE
==========

The data in now for sale. Anyone interested in the purchase should contact RansomHub. The data is for tens of insurance companies including and not limited to:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies

Data contains:
- Active US military/navy personnel PII/PHI
- Medical records (PHI)
- Dental records
- Payments information
- Claims information
- Patients PII/PHI including Phone numbers/addresses/SSN/emails/etc...
- thousand of source code files for Change Health solutions
- Insurance records
- And many more

Change Health and United Health processing of sensitive data for all of these companies is just something unbelievable. For most US individuals out there doubting us , we probably have your personal data.

292. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "dark web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The dark web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to

[158] Post by @BrettCallow, X (Apr. 16, 2024), https://x.com/BrettCallow/status/1780281243801878702.

trace. Tor uses a technique called "onion routing," where data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

293. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence. The anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Personal Information.[159]

294. Once stolen Personal Information is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[160]

295. This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and

[159] *Crime and the Deep Web*, Stevenson Univ., https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited Nov. 26, 2024); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a (last updated Aug. 2, 2021).
[160] *The Dark Web and Cybercrime*, U.S. Dep't of Health and Human Servs. (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf.

then "watermarked" it with their code that silently tracks any access to the file.[161] The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and Brazil, with the most activity coming from Nigeria and Russia.[162] This experiment demonstrated that data released on the dark web will quickly spread around the world.

III. Effects of the Data Breach

A. Defendants' customers face real, immediate, and significant harm

296. Personal Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[163] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Personal Information it collects about users of its various free products and services.

---

[161] Kelly Jackson Higgins, *What Happens When Personal Information Hits the Dark Web*, Dark Reading (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; Kristin Finklea, *Dark Web*, Nat'l Sec. Archive (July 7, 2015), https://nsarchive.gwu.edu/media/21394/ocr; *Dark Web*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R44101 (last updated Mar. 10, 2017).

[162] Pierluigi Paganini, *How Far Do Stolen Data Get in the Deep Web After a Breach?*, Security Affairs (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[163] *Alphabet Inc., Annual Report (Form 10-K)*, SEC, at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

297. Criminal law also recognizes the value of Personal Information and the serious nature of the theft of Personal Information by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Personal Information. Once a cybercriminal has unlawfully acquired Personal Information, the criminal can demand a ransom or blackmail payment for its destruction, use the Personal Information to commit fraud or identity theft, or sell the Personal Information to other cybercriminals on the black market.

298. The U.S. Government Accountability Office ("GAO") released a report as far back as 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[164] This has not changed over the nearly two decades since this study.

299. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name."

300. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[165] According to

[164] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[165] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or

Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[166]

301. With access to an individual's Personal Information, 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 Social Security number to obtain government benefits; filing a fraudulent tax return using the victim's information; or committing healthcare fraud using information related to an individual's health insurance. In addition, identity thieves may obtain a job using the victim's Social Security number, 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.[167]

---

in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[166] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[167] *Id.*

302. Identity theft presents many challenges. In a survey, the Identity Theft Resource Center ("ITRC") found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[168]

303. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new Social Security number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the victim experiences the harm.

304. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers 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.

305. Beyond monetary losses and healthcare fraud, data breaches also have a deep, psychological impact on their victims.

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you and prolong or worsen a cyber attack.[169]

306. Plaintiffs who have filed suit in this multidistrict litigation have suffered injuries in a number of ways, including:

---

[168] *ITRC Annual Data Breach Report 2023*, ITRC (2023), https://www.idtheftcenter.org/publication/2023-data-breach-report/.

[169] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

a. Loss of benefit of their bargain, for individuals who provided compensation to entities to safely transfer and store their data with one of the Defendants or Defendants' vendors;

b. Loss of value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;

c. Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as

d. Time and expenses that were reasonably spent to mitigate the impact of the breach, including the cost of credit monitoring.

307. Several Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, and which demonstrates that the Data Breach has put them at immediate risk for additional harm.

308. The fraud and attempted fraud that certain Plaintiffs have suffered is sufficiently related to the Data Breach because of the time frame in which it occurred (after the Data Breach), and because the same information that was exposed in the Data Breach would have been used to effectuate the fraud and identity theft.

309. The harm already suffered by Plaintiffs demonstrates that the risk of harm to Plaintiffs and Class members is present and ongoing.

B. It is reasonable for individual victims of data breaches to expend time and money to mitigate their risk of harm.

310. Cybercriminals can and do use the precise Personal Information that Defendants were entrusted to safeguard to perpetrate financial crimes that harm Plaintiffs and the Class members.

311. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their Personal Information after a data breach, including contacting one of the three credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[170]

312. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when 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."[171]

313. Personal Information is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

---

[170] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Nov. 26, 2024). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[171] GAO Report, supra, n.164.

314. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[172]

315. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[173] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use Personal Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[174] The FTC also warns, "[i]f the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[175]

316. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[176]

---

[172] Patrick Lucas Austin, "*It Is Absurd." Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[173] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[174] *See* FBI, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014) at 14, https://publicintelligence.net/fbi-health-care-cyber-intrusions/.
[175] *See* What to Know About Medical Identity Theft, FTC, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 26, 2024).
[176] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

317. A report published by the World Privacy Forum[177] and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services not sought or received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

318. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., donation history or hospital records), directly and

[177] Dixon & Emerson, supra, n.173.

materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[178]

319. The intent of hackers is clear when they hack systems such as the Defendants': they are attempting to access consumers' Personal Information for the purpose of ransoming it back and/or selling it for a profit.

320. Plaintiffs and Class members' stolen data will continue to be leaked and traded on the dark web, meaning Plaintiffs and Class members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class members are in the very early stages of their lives—in their twenties and thirties. Thus, as the respective Data Breach Notices advise, customers, including Plaintiffs and Class members, must vigilantly monitor their financial accounts for many years to come.

C. Damages can compensate victims for the harm caused by the Data Breach.

321. Defendants have refused to provide adequate compensation for Plaintiffs' and Class members' injuries.

[178] *See* Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

322. While Defendants have offered some credit monitoring, that is insufficient to remedy the harms caused by Defendants' Data Breach. A year or two of credit monitoring will not un-ring the bell of the release of the Personal Information of the Plaintiffs and Class members, which will circulate around the world and through the various levels of the internet (clear, dark, and deep) for years and years, if not in perpetuity. Particularly considering the fact that Social Security numbers were exposed in the Data Breach, Data Breach victims will need to monitor their credit and accounts for years and years to come—and these services are typically accounted for in settlements and judgments involving data breaches.[179]

323. Moreover, Defendants' offer of credit monitoring does not cover misuse of PHI. It is also predicated on Class members re-providing their Personal Information to Defendants' agents when Defendants themselves are responsible for the underlying Data Breach.

324. The Personal Information exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class members have therefore been deprived of their

[179] For instance, in July 2019, the CFPB, FTC, and States announced a settlement with Equifax over the 2017 Equifax data breach, which included up to ten years of credit monitoring and identity restoration services for victims. *See CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach*, CFPB (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

rights to control of that property and have lost the value they might otherwise have incurred from that data.[180]

325. Plaintiffs and the Class members have already spent significant time, and will spend much more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be compensated. Defendants have not made compensation or other remedies available for these very real injuries.[181]

326. Similarly, Defendants have offered no compensation for the aggravation, agitation, anxiety, and emotional distress that Plaintiffs and the Class members have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

327. Plaintiffs and Class members were also deprived of the benefit of their bargain when they interacted with Defendants: each Defendant had a duty to take reasonable steps to protect the Personal Information of the individuals whose information was entrusted to them and those individuals entrusted that information in exchange for Defendants taking on that duty. This duty was inherent in the relationships between

[180] Ravi Sen, *Here's How Much Your Personal Information Is Worth to Cybercriminals – and What They Do with It*, PBS (May 14, 2021), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[181] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited Nov. 26, 2024).

Plaintiffs and Class members and Defendants, whether through express contractual terms, implied contractual terms, or statutory or implied duties of good faith and fair dealing.

328. Defendants have not taken sufficient steps or even attempted to make impacted patients whole. Defendants have failed their duty to protect Plaintiffs' and Class members' Personal Information and have failed in their duty to help these consumers protect themselves in the future.

IV. UHG Defendants are responsible for Data Breach.

A. Defendants knew of the risks of data breaches.

329. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store private health information, preceding the date of the breach.

330. Attacks using stolen credentials have skyrocketed over the last several years.

331. Healthcare providers and their affiliates like Defendants are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and Personal Information of employees and patients—all extremely valuable on underground markets.

332. It is well known that use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

333. According to the FBI, phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of

cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[182] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[183]

334. The increased risk to healthcare entities was known and obvious to Defendants as they observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type they collect, maintain, and store is highly coveted and a frequent target of hackers.

335. There have been recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019, Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020).

---

[182] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited July 16, 2024).

[183] *2021 DBIR Master's Guide*, Verizon, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (last visited July 16, 2024).

336. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[184]

337. In addition, according to the 2023 ITRC Annual Data Breach Report, the number of data compromises in 2023 (3,205) increased by 78% compared to 2022 (1,801).[185] 2023 set a new record for the number of data compromises tracked in a year, up 72% from the previous all-time high in 2021 (1,860).[186]

338. Further, in Change Healthcare's SEC Form 10-K disclosures, it acknowledged the broad range of risks that are attributed to their field of business and its own company specifically. Change Healthcare claimed that:

a. Its services "involve the use and disclosure of personal and business information that could be used to impersonate third parties or otherwise gain access to their data or funds. If any of our employees or vendors or other bad actors takes, converts, or misuses such funds, documents or information, or we experience a data breach creating a risk of identity theft, we could be liable for damages, and our reputation could be damaged or destroyed;"[187]

b. It could "be perceived to have facilitated or participated in illegal misappropriation of funds, documents or data and, therefore, be subject to civil or criminal liability. Federal and state regulators may

[184] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (Jan. 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.
[185] ITRC, *supra* note 168.
[186] *Id.*
[187] *Change Healthcare Form 10-K* (Mar. 31, 2022), https://www.sec.gov/Archives/edgar/data/1756497/000175649722000007/chng-20220331x10k.htm.

take the position that a data breach or misdirection of data constitutes an unfair or deceptive act or trade practice;"[188]

c. "[D]espite [its] security management efforts […] [its] infrastructure, data or other operation centers and systems used in connection with [its] business operations, including the internet and related systems of [its] vendors are vulnerable to, and may experience, unauthorized access to data and/or breaches of confidential information due to criminal conduct;"[189] and

d. "[Its] products and services involve processing personal information. Like many organizations, [the UHG companies] have been and expect to routinely be the target of attempted cyber and other security threats by outside third parties, including technologically sophisticated and well-resourced bad actors attempting to access or steal the data [they] store."[190]

339. Similarly, UHG and Optum were well aware of both the foreseeable threat of a cyberattack and the consequences that would result from their failure to implement sufficient data security protections.

340. In UHG's SEC Form 10-K disclosures for the fiscal year ending December 31, 2023, which also analyzed and disclosed risks associated with Optum, UHG and Optum recognized that:

a. If we or third parties we rely on sustain cyber-attacks or other privacy or data security incidents resulting in disruption to our operations or the disclosure of protected personal information or proprietary or confidential information, we could suffer a loss of revenue and increased costs, negative operational affects, exposure to significant liability, reputational harm and other serious negative consequences.

b. We are regularly the target of attempted cyber-attacks and other security threats and have previously been, and may in the future be, subject to compromises of the information technology systems we

[188] *Id.*
[189] *Id.*
[190] *Id.*

use, information we hold, or information held on our behalf by third parties.

c. Threat actors and hackers have previously been, and may in the future be, able to negatively affect our operations by penetrating our security controls and causing system and operational disruptions or shutdowns, accessing, misappropriating or otherwise compromising protected personal information or proprietary or confidential information or that of third parties, and developing and deploying viruses, ransomware and other malware that can attack our systems, exploit any security vulnerabilities, and disrupt or shutdown our systems and operations.

d. There have previously been and may be in the future heightened vulnerabilities due to the lack of physical supervision and on-site infrastructure for remote workforce operations and for recently-acquired or non-integrated businesses. We rely in some circumstances on third-party vendors to process, store and transmit large amounts of data for our business whose operations are subject to similar risks.

e. [C]ompromises of our security measures or the unauthorized dissemination of sensitive personal information, proprietary information or confidential information about us, our customers or other third parties, previously and in the future, could expose us or them to the risk of financial or medical identity theft, negative operational affects, expose us or them to a risk of loss or misuse of this information, result in litigation and liability, including regulatory penalties, for us, damage our brand and reputation, or otherwise harm our business.[191]

341. Moreover, given the repeated warnings by government agencies and cybersecurity researchers to healthcare entities of the threat posed by ALPHV Blackcat, Defendants could and should have taken reasonable precautions against attacks such as this.

[191] *UnitedHealth Group Incorporated Form 10-K* (Feb. 28, 2024), https://www.sec.gov/Archives/edgar/data/1756497/000175649722000007/chng-20220331x10k.htm.

B. UHG Defendants breached their duties to prevent, monitor, identify, and fix security vulnerabilities in Change Healthcare's networks.

342. During a Senate hearing regarding the Data Breach, Senator Ron Wyden said the attack could have been stopped with 'Cybersecurity 101.'"[192] Indeed, as CEO Witty admitted, Change Healthcare lacked the necessary MFA on the server that was breached.[193]

343. Senator Thom Tillis further confirmed the preventability of this Data Breach. Waiving a copy of "Hacking for Dummies," Sen. Tillis emphasized that "[t]his is some basic stuff that was missed, so shame on internal audit, external audit and your systems folks tasked with redundancy, they're not doing their job[.]"[194]

344. Despite the foreseeability of the Data Breach, this cyber disaster occurred in part because, as CEO Witty highlighted, Change Healthcare is a 40-year-old company with outdated and differing generations of technology.[195]

345. Change Healthcare's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred.

---

[192] Pietje Kobus, *UnitedHealth CEO Testifies on Cyberattack Before Senate*, Healthcare innovation (May 2, 2024), https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate.

[193] *Id.*

[194] Ashley Capoot, *UnitedHealth CEO Tells Lawmakers the Company Paid Hackers a $22 Million Ransom*, CNBC (May 1, 2024), https://www.cnbc.com/2024/05/01/unitedhealth-ceo-says-company-paid-hackers-22-million-ransom.html.

[195] Gopal Ratnam, *Change Healthcare lacked safeguards even as it gave security advice*, Roll Call (May 7, 2024, 7:00 AM), https://rollcall.com/2024/05/07/change-healthcare-lacked-safeguards-even-as-it-gave-security-advice/.

346. However, by marketing and advertising the Change Platform as a solution for handling highly sensitive Personal Information, Defendants assumed legal and equitable duties and knew or should have known it was responsible for:

a. adequately designing, maintaining, and updating their software and networks;

b. promptly detecting, remediating, and notifying their customers of any critical vulnerabilities in their software and networks;

c. ensuring compliance with industry standards related to data security;

d. ensuring compliance with regulatory requirements related to data security;

e. protecting and securing the Personal Information stored on their networks from unauthorized disclosure; and

f. providing adequate notice to customers and individuals if their Personal Information is disclosed without authorization.

347. Defendants failed to use the requisite degree of care that a reasonably prudent company would use in designing, developing, and maintaining networks that store highly sensitive Personal Information.

348. Defendants should have implemented industry standard security protocols to mitigate the risk of stolen credentials, including MFA and internal cybersecurity monitoring.

349. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making

employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

350. User education provides the easiest method to assist in properly identifying fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[196]

351. Companies can also take steps to ensure that user passwords are not recycled across platforms, so that a breach, for example, of a user's Netflix password would not yield a password that could also be used to access that user's work account at Change Healthcare.

[196] *Ransomware Guide*, Multi-State Information Sharing & Analysis Center, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

352. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

a. Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

b. Regularly patching and updating software to the latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

c. Ensuring devices are properly configured and that security features are enabled;

d. Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

e. Disabling operating system network file sharing protocol known as Server Message Block (SMB), which is used by threat actors to travel through a network to spread malware or access sensitive data.[197]

353. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[198] Likewise, the principle of

[197] *Id.* at 4.
[198] *Id.* at 5.

least privilege ("POLP") should be applied to all systems so that users only have the access they need to perform their jobs.[199]

354. Not only should Defendants have had measures like these in place to prevent compromise in the first place, Defendants should have also properly siloed their systems so that a bad actor would be unable to escalate privileges and move laterally through Defendants' systems.

355. A data silo can occur when an organization manages data separately without maintaining a centralized system to share and information. For example, once Change Healthcare's system was infiltrated, ALPHV was able to disable both the primary and backup systems because the backup systems were not isolated from the primary and few elements were stored on the cloud, both basic security features.

356. Similarly, the lack of segmented systems, which are common to cloud-based servers, allowed the hacker to travel among Change Healthcare's systems freely, compromising multiple systems which Change Healthcare was unable to recover, and ultimately resulting in the complete shutdown of Change Healthcare's operations.

357. CISA guidance recommends that using a comprehensive network, in addition to network segregation, will help contain the impact of an intrusion and prevent or limit lateral movement on the part of malicious actors.

358. Despite holding the PII and PHI of millions of patients, Defendants failed to adhere to these recommended best practices. Indeed, had Defendants implemented

[199] *Id.* at 6.

common sense security measures like MFA, the hackers never could have accessed millions of patient files and the Data Breach would have been prevented or been much smaller in scope. Defendants also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

359. Defendants, like any entity in the healthcare industry their size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Defendants' below-industry-standard procedures and policies are inexcusable given their knowledge that they were a prime target for cyberattacks.

360. To the extent UHG Defendants required MFA in any of its internal policies, procedures, or protocols, they should have ensured MFA was in fact implemented throughout its system.

361. UHG Defendants' failure to follow industry standard cybersecurity protocols directly resulted in the Data Breach and the compromise of Plaintiffs and Class members' Personal Information.

V. Defendants failed to follow industry standards for data security

A. FTC guidelines

362. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[200]

363. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal health information that they keep; properly dispose of patient information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[201]

364. The guidelines also recommend that healthcare businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[202]

---

[200] *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[201] *Protecting Personal Information: A Guide for Business,* FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[202] *Id.*

365. The FTC further recommends that healthcare companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

366. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[203]

367. Defendants were fully aware of their obligation to implement and use reasonable measures to protect the Personal Information of their patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Defendants' failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[203] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Jan. 13, 2025).

B. HIPAA obligations

368. Defendants are covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

369. These rules establish national standards for the protection of patient information, including personal health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

370. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[204]

371. HIPAA requires that Defendants implement appropriate safeguards for this information.[205]

372. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not

[204] 45 C.F.R. § 164.502.
[205] 45 C.F.R. § 164.540(c)(1).

rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e., non-encrypted data.[206]

373. CISA and HIPAA also require that the principle of least privilege ("POLP") be applied to all systems so that users only have the access they need to perform their jobs.[207] HIPAA refers to this as the "Minimum Necessary Rule."[208] Other applicable standards also require *least privileges*, such as *PCI-DSS requirement 7,* which requires least privileges.[209] NIST 800-53 also requires adherence to the principle of least privileges.[210]

---

[206] 45 C.F.R. §§ 164.402, 404.

[207] *Ransomware Guide*, Multi-State Information Sharing & Analysis Center, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

[208] Steve Alder, *The HIPAA Minimum Necessary Rule Standard*, The HIPAA Journal (Dec. 5, 2024), https://www.hipaajournal.com/ahima-hipaa-minimum-necessary-standard-3481/; *Minimum Necessary, FAQs*, U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/minimum-necessary/index.html (last visited Jan. 2, 2025).

[209] *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.1*, PCI Security Standards Council (May 2015), https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf; Surkay Baykara, *PCI DSS Requirement 7 Explained*, PCI DSS Guide (Apr. 7, 2020), https://pcidssguide.com/pci-dss-requirement-7/; *How to Comply with PCI DSS Compliance Requirement 7*, Indent (Dec. 6, 2023), https://indent.com/blog/pci-dss-requirement-7.

[210] Tony Goulding, *What you need to know about NIST 800-53, least privilege, and PAM*, Delinea, https://delinea.com/blog/nist-800-53-security-privacy-privileged-access (last visited Jan. 2, 2025); *NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf (last visited Jan. 2, 2025); Asif Ali, *What you need to know about NIST 800-53, least privilege, and PAM*, AuthNull, https://authnull.com/blog/posts/What-you-need-to-know-about-NIST-800-53,-least-privilege,-and-PAM/ (last updated Sept. 8, 2024).

374. The account of the low-level employee that was compromised to access Defendants' system should not have been configured in such a way as to allow it to create accounts with administrative privileges that could in turn be used to access and exfiltrate Personal Information. This is clear evidence Change Healthcare did not follow the principle of least privilege or the Minimum Necessary Rule.

375. Had Defendants adequately implemented policies and procedures applying the principle of least privilege or the Minimum Necessary Rule, the Data Breach and theft of Plaintiffs' and Class members' Personal Information could have been prevented.

376. HIPAA further requires covered entities to "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."[211] MFA is widely recommended to meet this requirement for all healthcare applications,[212] and there are a number of services that can handle the MFA for an organization.[213] The book *HIPAA Privacy and Security Compliance – Simplified: Practical*

[211] 45 C.F.R. § 164(c).

[212] Marty Puranik, *Two-Factor Authentication: A Top Priority for HIPAA Compliance*, Techopedia (Aug. 25, 2023), https://www.techopedia.com/two-factor-authentication-a-top-priority-for-hipaa-compliance/2/33761; *Utilizing Two Factor Authorization*, HHS Cybersecurity Program, Office of Information Security, https://www.hhs.gov/sites/default/files/two-factor-authorization.pdf (last visited Jan. 2, 2025); Liyanda Tembani, *Enhancing HIPAA compliance with multi-factor authentication*, Paubox (Aug. 9, 2024), https://www.paubox.com/blog/enhancing-hipaa-compliance-with-multi-factor-authentication; Gil Vidals, *Multi-Factor Authentication For HIPAA Compliance: Securing Patient Data In The Digital Age*, HIPAAVault (Dec. 6, 2023), https://www.hipaavault.com/hipaa-outlook/multi-factor-authentication-for-hipaa-compliance/.

[213] *Healthcare*, Okta, https://www.okta.com/solutions/healthcare/ (last visited Jan. 2, 2025); *Build vs. Buy for Healthcare: A Healthcare Guide for Identity Whitepaper*, Auth0 by Okta, https://auth0.com/resources/whitepapers/build-vs-buy-for-healthcare (last visited Jan. 2, 2025).

Guide for Healthcare Providers and Managers states "Multi-factor authentications (MFA) shall be used for remote access, for system administration activities and for access to critical systems."[214]

377. MFA is also required by a number of other industry standards:

a. The Payment Card Industry Data Security Standard PCI-DSS requires multi-factor authentication per requirement 8.2[215].

b. Service Organization Control 2 (SOC 2) a widely used cybersecurity auditing standard used for a wide range of businesses, requires multi-factor authentication[216].

c. ISO 27002 is an international standard that provides guidance for organizations on how to establish, implement, and improve an Information Security Management System. ISO 27002 requires one to either use MFA, digital certificates, smart cards, or biometric login[217].

---

[214] Robert Brzezinski, *HIPAA Privacy and Security Compliance - Simplified: Practical Guide for Small and Medium Organizations* 47 (2016 ed.).
[215] *Information Supplement: Multi-Factor Authentication*, PCI Security Standards Council (Feb. 2017), https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf.
[216] Joe Ciancimino, *Comprehensive Guide to SOC 2 Controls List*, ISPartners (Nov. 2, 2023), https://www.ispartnersllc.com/blog/soc-2-controls/.
[217] *ISO 27002:2022.Control 8.5 -Secure Authentication*, ISMS Online, https://www.isms.online/iso-27002/control-8-5-secure-authentication/ (last visited Jan. 2025).

d. The Cybersecurity and Infrastructure Security Agency has strongly encouraged all businesses to use MFA for many years[218].

e. NIST 800-53 is a cybersecurity framework and compliance standard that can be used by any organization. NIST 800-53 strongly recommends MFA beginning on page 132[219].

378. HIPAA security standards require organizations to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[220] Automatically tracking IoC's, such as those released by the FBI regarding ALPHV in April 2022, is a recommended practice.[221]

379. It is also recommended to use an Intrusion Prevention System (IPS) and in order "[t]o stay up to date, IPS should leverage a Structure Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) feed to obtain IOC from an Information Sharing and Analysis Center (ISAC) or similar source."[222]

---

[218] *Require Multifactor Authentication*, CISA DHS, https://www.cisa.gov/secure-our-world/require-multifactor-authentication (last visited Jan. 13, 2025).
[219] *NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last visited Jan. 2, 2025).
[220] 45 C.F.R. § 164.306.
[221] Robert Brzezinski, *HIPAA Privacy and Security Compliance - Simplified: Practical Guide for Small and Medium Organizations* 28 (2016 ed.)
[222] *Technical Vol. 2: Cybersecurity Practices for Medium and Large Healthcare Organizations 2023 Edition*, Healthcare & Public Health Sector Coordinating Council, U.S. Dept. of Health & Human Services, https://405d.hhs.gov/Documents/tech-vol2-508.pdf (last visited Jan. 2, 2025).

380. Having systems in place for continuous monitoring for IoCs is also recommended.[223]

381. As evidenced by the Data Breach, Defendants did not track IoCs regarding ALPHV.

382. Despite the requirements under HIPAA for data security, Defendants failed to comply with their duties under HIPAA and their own privacy policies. Indeed, Defendants failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the Personal Information of patients;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

[223] *SecurityMetrics Guide to HIPAA Compliance*, SecurityMetrics (8th ed. 2023), ("Automating log collection, correlation and review to Detect Indicators of Attack (IoA) and Indicators of Compromise (IoC). Security Incident and Event Management (SIEM) tools are a good way to automate the process even for small companies.").

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

383. NIST 800-53 also recommends removing, masking, encrypting, or hashing PII contained in company datasets.[224]

> There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that

[224] *NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last visited Jan. 2, 2025).

> the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming "George Washington" to "PATIENT" or replacing it with a surrogate value, such as transforming "George Washington" to "Abraham Polk."[225]

384. Given the attackers were able to access Personal Information simply by logging in, it is clear that Defendants did not protect Plaintiffs' and Class members' Personal Information with sufficient masking, encrypting, or hashing.

385. Defendants were fully aware of their obligations to implement and use reasonable measures to protect the Personal Information of patients but failed to comply with these basic recommendations and guidelines that would have prevented this Data Breach from occurring. Defendants' failure to employ reasonable measures to protect against unauthorized access to patient Personal Information violated HIPAA and constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

CLASS ALLEGATIONS

386. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (23(b)(3), individually and on behalf of all members of the following nationwide class:

> **Nationwide Class:** All residents of the United States and its Territories who had their Personal Information compromised due to the Data Breach.

[225] *Id.*

387. Plaintiffs also bring their causes of action on behalf of themselves and on behalf of residents of the same state as each Plaintiff that belong to the following state sub-classes (collectively, "Subclasses"):

> **Alabama Subclass:** All residents of Alabama who had their Personal Information compromised due to the Data Breach.
>
> **Alaska Subclass:** All residents of Alaska who had their Personal Information compromised due to the Data Breach.
>
> **Arizona Subclass:** All residents of Arizona who had their Personal Information compromised due to the Data Breach.
>
> **Arkansas Subclass:** All residents of Arkansas who had their Personal Information compromised due to the Data Breach.
>
> **California Subclass:** All residents of California who had their Personal Information compromised due to the Data Breach.
>
> **Colorado Subclass:** All residents of Colorado who had their Personal Information compromised due to the Data Breach.
>
> **Connecticut Subclass:** All residents of Connecticut who had their Personal Information compromised due to the Data Breach.
>
> **Delaware Subclass:** All residents of Delaware who had their Personal Information compromised due to the Data Breach.
>
> **Florida Subclass:** All residents of Florida who had their Personal Information compromised due to the Data Breach.
>
> **Georgia Subclass:** All residents of Georgia who had their Personal Information compromised due to the Data Breach.
>
> **Hawaii Subclass:** All residents of Hawaii who had their Personal Information compromised due to the Data Breach.
>
> **Idaho Subclass:** All residents of Idaho who had their Personal Information compromised due to the Data Breach.

Illinois Subclass: All residents of Illinois who had their Personal Information compromised due to the Data Breach.

Indiana Subclass: All residents of Indiana who had their Personal Information compromised due to the Data Breach.

Iowa Subclass: All residents of Iowa who had their Personal Information compromised due to the Data Breach.

Kansas Subclass: All residents of Kansas who had their Personal Information compromised due to the Data Breach.

Kentucky Subclass: All residents of Kentucky who had their Personal Information compromised due to the Data Breach.

Louisiana Subclass: All residents of Louisiana who had their Personal Information compromised due to the Data Breach.

Maine Subclass: All residents of Maine who had their Personal Information compromised due to the Data Breach.

Maryland Subclass: All residents of Maryland who had their Personal Information compromised due to the Data Breach.

Massachusetts Subclass: All residents of Massachusetts who had their Personal Information compromised due to the Data Breach.

Michigan Subclass: All residents of Michigan who had their Personal Information compromised due to the Data Breach.

Minnesota Subclass: All residents of Minnesota who had their Personal Information compromised due to the Data Breach.

Mississippi Subclass: All residents of Mississippi who had their Personal Information compromised due to the Data Breach.

Missouri Subclass: All residents of Missouri who had their Personal Information compromised due to the Data Breach.

Montana Subclass: All residents of Montana who had their Personal Information compromised due to the Data Breach.

Nebraska Subclass: All residents of Nebraska who had their Personal Information compromised due to the Data Breach.

Nevada Subclass: All residents of Nevada who had their Personal Information compromised due to the Data Breach.

New Hampshire Subclass: All residents of New Hampshire who had their Personal Information compromised due to the Data Breach.

New Jersey Subclass: All residents of New Jersey who had their Personal Information compromised due to the Data Breach.

New Mexico Subclass: All residents of New Mexico who had their Personal Information compromised due to the Data Breach.

New York Subclass: All residents of New York who had their Personal Information compromised due to the Data Breach.

North Carolina Subclass: All residents of North Carolina who had their Personal Information compromised due to the Data Breach.

North Dakota Subclass: All residents of North Dakota who had their Personal Information compromised due to the Data Breach.

Ohio Subclass: All residents of Ohio who had their Personal Information compromised due to the Data Breach.

Oklahoma Subclass: All residents of Oklahoma who had their Personal Information compromised due to the Data Breach.

Oregon Subclass: All residents of Oregon who had their Personal Information compromised due to the Data Breach.

Pennsylvania Subclass: All residents of Pennsylvania who had their Personal Information compromised due to the Data Breach.

Rhode Island Subclass: All residents of Rhode Island who had their Personal Information compromised due to the Data Breach.

South Carolina Subclass: All residents of South Carolina who had their Personal Information compromised due to the Data Breach.

South Dakota Subclass: All residents of South Dakota who had their Personal Information compromised due to the Data Breach.

Tennessee Subclass: All residents of Tennessee who had their Personal Information compromised due to the Data Breach.

Texas Subclass: All residents of Texas who had their Personal Information compromised due to the Data Breach.

Utah Subclass: All residents of Utah who had their Personal Information compromised due to the Data Breach.

Vermont Subclass: All residents of Vermont who had their Personal Information compromised due to the Data Breach.

Virginia Subclass: All residents of Virginia who had their Personal Information compromised due to the Data Breach.

Washington Subclass: All residents of Washington who had their Personal Information compromised due to the Data Breach.

West Virginia Subclass: All residents of West Virginia who had their Personal Information compromised due to the Data Breach.

Wisconsin Subclass: All residents of Wisconsin who had their Personal Information compromised due to the Data Breach.

Wyoming Subclass: All residents of Wyoming who had their Personal Information compromised due to the Data Breach.

388. Excluded from the Class and Subclasses are Defendants' officers and directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

389. Plaintiffs reserve the right to amend or modify the Class and Subclass definitions.

390. **Numerosity**. The Class and each Subclass are so numerous that joinder is impracticable. While the exact number of Class members is unknown to Plaintiffs, Defendants have confirmed that the Class consists of over one-hundred million United States residents residing in each State, totaling over one-third of the United States.

391. **Commonality**. There are questions of law and fact common to the Class and each Subclass, which predominate over any questions affecting only individual Class and Subclass members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs and Class and Subclass members' Personal Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards and state and federal regulatory requirements, including HIPAA;

e. Whether Defendants were subject to and breached contractual obligations to adhere to HIPAA in their business association agreements;

f. Whether Defendants owed a duty to Class and Subclass members to safeguard their Personal Information;

g. Whether Defendants breached their duties to Class and Subclass members to safeguard their Personal Information;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Defendants should have discovered the Data Breach earlier;

j. Whether Defendants delay in issuing notice to Plaintiffs and the Class and Subclass caused them incremental harm;

k. Whether Plaintiffs and Class and Subclass members suffered legally cognizable damages as a result of Defendants' misconduct;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner;

n. Whether Defendants were unjustly enriched due to their use of Plaintiffs' and the Class's Personal Information while failing to protect it; and,

o. Whether Plaintiffs and Class and Subclass members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

392. **Typicality**. Plaintiffs' claims are typical of those of other Class and Subclass members because Plaintiffs' Personal Information, like that of every other Class and Subclass member, was compromised in the Data Breach, causing them common injury, which was due to the same misconduct—Defendants' inadequate data security.

393. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class and Subclass members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

394. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiffs and Class and Subclass members, in that all of Plaintiffs' and Class Subclass members' Personal Information was stored on the same computer system and unlawfully accessed by authorized users in the same way due to the same security deficiencies. Defendants' misconduct caused common injuries that affect all Class and Subclass members. Defendants' common course of wrongdoing and the common, classwide injuries create common legal and factual issues that predominate over any individualized issues. Adjudication of these common issues in a single action advances the interests of judicial economy.

395. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation concerning the same facts and law. Moreover, this case furthers the quintessential purpose of a class action, which is to afford Class and Subclass members with common injuries to pursue collective litigation where their individual damages are small. Given the size of the Plaintiffs' and Class and Subclass members' individual damages, the costs of individual litigation would likely exceed any award, leaving Plaintiffs and Class and Subclass members with effectively no remedy for their harm. Additionally, the prosecution of separate actions by individual Class and Subclass members would create a risk of

inconsistent or varying adjudications and establish incompatible standards of conduct for healthcare entities. In contrast, litigating this matter as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class member.

396. Defendants have acted on grounds that apply generally to the Class and Subclass as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I

Negligence

(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

397. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

398. From 2012 to the present, Defendants, via their business operations, collected, maintained, stored, used, analyzed, and processed Plaintiffs' and the Class's highly private information, including personally identifying and medical information. Specifically, Defendants operated as a single unit to collect medical information from providers (through Change Healthcare's insurance processing), provide data analytics on the medical information (through Optum and Optum Insight's services), and inform insurance risks (through UHC's insurance offerings). The goal of those separate activities was, ultimately, to further UHG's profit and gain an advantage against its competitors.

399. Defendants understood the need to adequately protect that sensitive information and the serious risk a data breach poses to patients, such as Plaintiffs and the Class. Andrew Witty, UHG's CEO, testified that he agreed UHG has an "obligation to protect [patient] information" and that it "take[s] that obligation very seriously." Witty also testified that UHG experiences "a cybersecurity attempted attack every 70 seconds," acknowledging that patient information stored with Defendants remains at constant risk. Each Defendant, furthermore, was subject to state and federal regulations, including HIPAA and state-law equivalents, that required each Defendant to implement reasonable physical, technical, and administrative safeguards to protect patient information from unauthorized access, use, or disclosure.

400. Further, given the value of patient data to Defendants and their business model and the well-known misuse of patient information by cybercriminals, Defendants also fully understood that patient data has significant monetary value. Defendants knew or should have known that, should that sensitive data be accessed by unauthorized users, it would likely be sold on the dark web to fraudsters, putting patients, including Plaintiffs and the Class, at significant risk that their Personal Information would be used for fraudulent purposes. Indeed, the sole fact that Defendants *themselves* profited from the data that comprises Plaintiffs' and the Class's Personal Information demonstrates that Defendants knew or should have known the importance of data security.

401. Given the highly sensitive nature of the data, and the foreseeable risk of a Data Breach, Defendants, each individually and collectively, owed Plaintiffs and the Class a duty to exercise reasonable care in securing the highly sensitive Personal Information,

including a host of private medical data, that Defendants collected, maintained, stored, used, analyzed, and processes as part of their businesses.

402. Defendants owed this duty to Plaintiffs and the Class because Plaintiffs and the Class are a well-defined, and foreseeable group of individuals whom Defendants should have been aware could be injured by Defendants' inadequate data storage and security. The foreseeable harm to Plaintiffs and the Class of Defendants' inadequate data security measures and the fact that Defendants were the only entities capable of protecting Plaintiffs' and the Class's data within their possession created a duty to act reasonably in securing Personal Information.

403. Additionally, Defendants assumed a duty to Plaintiffs and the Class to protect their sensitive Personal Information. Defendants represented to providers and others that they would comply with HIPAA to implement measures to reasonably safeguard the patient information within their possession. As such, when healthcare providers and other intermediaries provided Defendants with Plaintiffs' and the Class's Personal Information and Defendants accepted and stored that data (for their own purposes and to their own financial benefit), Defendants assumed a duty to protect that Personal Information.

404. Defendants also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the Class can take appropriate measures to avoid unauthorized use of their Personal Information and accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring

services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendants' unreasonable misconduct.

405. Each Defendant, furthermore, owed a duty individually. Change Healthcare and Optum Insights, which merged with Change Healthcare, took actions that created a risk of harm, triggering a duty to correct the risk their actions created. Change Healthcare, prior to and after its merger with Optum Insights, collected and stored highly sensitive information in plaintext (*i.e.*, in an unencrypted format), retained decades' old data without disposal, and implemented inadequate data security, including failing to put in place even basic multi-factor authentication to restrict access to patient data.

406. Optum, furthermore, took responsibility for securing the data contained within Change Healthcare. For instance, in explaining how "patient specific data and information [is] protected by Optum," Optum promised to "safeguard patient data and information" obtained via Change Healthcare.

407. Finally, UHG retained control and oversight over cybersecurity amongst its subsidiaries, including Change Healthcare. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and state that it took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to meet. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other actions,

constantly assessing and improving capabilities, working with key technology partners, sharing information about security threats and best practices, running continuous penetration tests, and providing external support to Change Healthcare. Andrew Witty also stated that UHG's experienced Board of Directors "oversee[s] the program," including "risk management" and "cybersecurity," and that its Audit and Finance Committee "oversees cybersecurity risks." Demonstrating its control, UHG took control over responsibility for investigating and responding to the Data Breach.

408. Consequently, each Defendant owed Plaintiffs and the Class a duty to reasonably secure Plaintiffs' and the Class's Personal Information held by Change Healthcare and obtained by UHG and Optum upon its acquisition of Change Healthcare.

409. Despite that duty, Defendants did not implement reasonable data security and negligently maintained Plaintiffs' and the Class's Personal Information. For example, Defendants failed to implement multi-factor authentication on remote accounts with access to Change Healthcare's legacy servers; lacked internal cybersecurity monitoring of Change Healthcare's systems; and failed to adequately segregate sensitive information from Change Healthcare's other systems. Each of these failures contravenes well-established, basic industry standards, expert recommendations, and basic requirements for reasonable data security.

410. Defendants knew that their failure to use reasonable measures to protect Class members' Personal Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the well-known high frequency of cyberattacks and data breaches in the past few years.

411. Defendants' negligent data security actually and proximately caused Plaintiffs' and the Class's injuries because they directly allowed hackers to easily access Plaintiffs' and the Class's Personal Information. This ease of access allowed the hackers to steal Personal Information of Plaintiffs and the Class, resulting in the dissemination of that data on the dark web.

412. As a direct and proximate result of Defendants' misconduct, Plaintiffs and the Class have suffered theft of their Personal Information. Defendants allowed cybercriminals to access Class members' Personal Information, thereby decreasing the security of the Class's financial and health accounts, making Class members' identities less secure and reliable, and subjecting the Class to the imminent threat of identity theft. Not only will Plaintiffs and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

413. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense

responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

414. Plaintiffs and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Plaintiffs and the Class. Without the use of adequate data security, Plaintiffs and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

415. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and which the court deems proper.

COUNT II

Negligence *Per Se*

(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

416. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

417. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Personal Information. 15 U.S.C. § 45.

418. Plaintiffs and Class members are within the class of persons that the FTCA was intended to protect.

419. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses that, due to their failure to employ reasonable data security measures and abstain from unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class here.

420. As entities that receive patient information, Defendants are "business associates" under HIPAA. Business associates have legal obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into business associate agreements ("BAAs") between business associates and covered entities); see also 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.

421. Plaintiffs and the Class, as patients, are within the class of people HIPAA was designed to protect and HIPAA was intended to protect Plaintiffs and the Class against the type of harm that occurred, namely, unauthorized access to Plaintiffs' and the Class's medical information.

422. Defendants' implementation of inadequate data security failed to comply with HIPAA, including because it: (i) failed to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the Class's Personal Information; (ii) failed

to adequately monitor Change Healthcare's servers despite the vast amount of patient data stored there; (iii) failed to implement multi-factor authentication on remote access accounts; (iv) allowed unauthorized access to Plaintiffs' and the Class's Personal Information; (iv) failed to detect in a timely manner the unauthorized access and exfiltration of patient data occurring in Change Healthcare's systems; and (v) failed to timely and adequately notify Plaintiffs' and the Class of the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

423. Defendants knew that their inadequate data security measures put Plaintiffs and the Class at foreseeable risk of harm from a data breach (including the Data Breach described in this Consolidated Complaint) which, in turn, put Plaintiffs at risk of harm due to the theft and misuse of their data.

424. As a direct and proximate result of Defendants' misconduct, Plaintiffs and the Class have suffered theft of their Personal Information. Defendants' allowed cybercriminals to access Class members' Personal Information, thereby decreasing the security of the Class's financial and health accounts, making Class members' identities less secure and reliable, and subjecting the Class to the imminent threat of identity theft. Not only will Plaintiffs and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

425. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries,

including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

426. Plaintiffs and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Plaintiffs and the Class. Without the use of adequate data security, Plaintiffs and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

427. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT III

Third Party Beneficiary – Breach of Contract

(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

428. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

429. Under HIPAA, a "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provider of certain services to, a covered entity that involve access by the business associate to PHI. HIPAA rules require that a covered entity and any business associate enter into an agreement (called a BAA, further described below) requiring the business associate to appropriately safeguard PHI.

430. Pursuant to HIPAA, a "business associate must comply with the applicable standards, implementation specifications, and requirements of [HIPAA] with respect to electronic protected health information of a covered entity." 45 C.F.R. § 164.302. Those safeguards include obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902. These requirements are uniform and exist in every BAA.

431. Because each Defendant uses, analyzes, collets, obtains and accesses personal health information of patients, each must enter into Business Association Agreements ("BAA") with a covered entity, intermediatory, or other third party from whom Defendants obtain medical information. Through the normal course of their business, each Defendant obtains and uses personal health information, including Plaintiffs' and the Class's Personal Information. Consequently, to have obtained access to and used Plaintiffs' and the Class's Personal Information, each Defendant must have entered into one or more BAA with one or more covered entities.

432. Those BAAs must each contain identical requirements obligating the signatories (*i.e.*, here, Defendants) to comply with HIPAA. The requirements in the BAA are intended to protect patients like Plaintiffs' and the Class against the disclosure, theft, unauthorized access, or other harms stemming from the use of their medical information.

433. Although each Defendant was subject to a BAA and, therefore, HIPAA's requirements to implement adequate safeguards to protect patient information, Defendants failed to comply. Specifically, Defendants violated HIPAA and, thereby, breached their BAAs by, among other things, failing to adequately secure Plaintiffs' and the Class's Personal Information, and failing to implement reasonable administrative, technical, and physical safeguards to protect Plaintiffs' and the Class's Personal Information. Among other things, Defendants violated HIPAA by permitting access to servers containing Plaintiffs' and the Class's unencrypted Personal Information without the use of MFA; failed to adequately segregate Plaintiffs' and the Class's Personal Information; and failed

to adequately monitor activity on the sever containing Plaintiffs' and the Class's Personal Information.

434. As a direct and proximate result of Defendants' violation of HIPAA and breach of its required BAAs, Plaintiffs and the Class suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

435. Plaintiffs and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Plaintiffs and the Class via the direct or indirect contracts with providers. Absent compliance to those contracts' data security requirements, Plaintiffs and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

436. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs;

reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT IV

Unjust Enrichment

(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

437. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

438. Defendants received a substantial monetary benefit from Plaintiffs and the Class by the collection, maintenance, and use (for their own benefit) of Plaintiffs' Personal Information. Defendants have made substantial gains through the collection and analysis of Plaintiffs' and the Class's Personal Information, which Defendants obtained under the promise of securing patient data from unauthorized access and to comply with HIPAA and other state and federal requirements to implement reasonable measures to protect that Personal Information.

439. Specifically, Change Healthcare and Optum Insight derived value by collecting, using, analyzing Plaintiffs' and the Class's Personal Information. Change Healthcare and Optum Insight sold the information and analyses of it to other entities, thereby deriving a substantial benefit. Both entities, without any knowledge of the Plaintiffs and the Class, had unfettered rights to use Plaintiffs' and the Class's Personal Information for its own business profit.

440. Similarly, Optum and UHG profited from the use, sale, and analysis of Plaintiffs' and the Class's Personal Information, which they used to maximize profit,

increase their ability to compete with competitors, and obtain additional revenue at the expense of patients like Plaintiffs and the Class.

441. Furthermore, each entity, all of which took responsibility for securing Plaintiffs' and the Class's Personal Information, saved money by: (1) devoting knowingly inadequate resources to securing Change Healthcare's servers and networks despite its knowledge that the servers were out of data and lacked adequate protections; and (2) prioritizing rebuilding the Change Platform after the Data Breach rather than timely notifying Plaintiffs and the Class that their Personal Information was impacted in the Data Breach, preventing Plaintiffs and the Class for taking measures to protect against harm stemming from the misuse of their data.

442. Defendants would be unable to engage in their regular course of business without collecting the Personal Information from Plaintiffs' and the Class's medical providers.

443. Defendants' acceptance of the benefits of Plaintiffs' and the Class's Personal Information under the facts and circumstances is unfair, unjust, and inequitable.

444. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class members.

445. If Plaintiffs and Class members knew that Defendants had not secured their Personal Information or that they used their private medical information for their own financial gain, Plaintiffs and the Class would not have agreed to allow their providers to send their medical information to Defendants or to make unfettered use of that information, all while failing to implement reasonable safeguards to protect it.

446. Plaintiffs and Class members have no adequate remedy at law.

447. Due to Defendants' unjust enrichment, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

448. Plaintiffs and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Plaintiffs and the Class. Without the use of adequate data security requirements, Plaintiffs and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

449. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from the use of Plaintiffs and the Class's Personal Information.

COUNT V

Declaratory Judgment

(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

450. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

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

452. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Personal Information and whether Defendants currently maintain data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Personal Information.

453. Plaintiffs allege that Defendants' data security measures remain inadequate. Plaintiffs and Class members will continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

454. That risk stems from Defendants' retention of Plaintiffs' Personal Information, and its continued collection and aggregation of new medical information in the normal course of business through Change Healthcare's processing and resolution of

insurance claims. Defendants, thus, will continue to receive new and additional medical information concerning Plaintiffs and the Class and, consequently, Plaintiffs and the Class remain at substantial risk of a subsequent breach resulting in the theft of additional Personal Information.

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

a. Defendants continue to owe a legal duty to secure Plaintiffs' and Class members' Personal Information and to timely notify Plaintiffs and Class members of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes.

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class members' Personal Information.

456. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' Personal Information.

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

458. The hardship to Plaintiffs and Class members, if an injunction does not issue, exceeds the hardship to Defendants if an injunction is issued. Among other things, if

another data breach occurs at Defendants, Plaintiffs and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

459. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiffs and the Class whose Personal Information would be further compromised.

COUNT VI

Violation of AL ST § 8-19-1, et seq. ("DTPA"),

(On behalf of Alabama Plaintiffs and the Alabama Subclass against all Defendants)

460. Alabama Plaintiffs, individually and on behalf of the Alabama Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

461. Alabama's Deceptive Trade Practices Act (DTPA) prohibits any person from "engaging in any… unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce." AL ST § 8-19-5 (27).

462. Defendants violated the DTPA by engaging in conduct that constituted "unconscionable acts or practices in the conduct of trade or commerce.

463. Specifically, Defendants collected and stored Plaintiffs' and the Alabama Subclass's Personal Information. Defendants stored the Personal Information in a

knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' the Alabama Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

464. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without two-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of two factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

465. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes an immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people, including Alabama Plaintiffs and the Alabama Subclass. That is especially true because, despite failing to reasonably protect Alabama Plaintiffs' and the Alabama Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Alabama Plaintiffs'

and the Alabama Subclass's Personal Information. While Defendants profited off of Plaintiffs' and the Class's data, they failed to take the necessary measures to protect it, leaving Alabama Plaintiffs and the Alabama Subclass at significant and foreseeable risk of harm.

466. Although Defendants collectively acted in violation of the DTPA, each Defendant also separately violated the DTPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change, violated the DTPA by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

467. Optum also independently violated the DTPA. Upon its acquisition of Change Healthcare, Optum oversaw Change and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control

over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

468. Lastly, UHG also independently violated the DTPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

469. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

470. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Alabama Subclass at significant risk of harm.

471. Consequently, Defendants collectively and each independently took actions in violation of the DTPA.

472. As a result of those unlawful and unfair business practices, Plaintiffs and the Alabama Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

473. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity,

name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

474. Alabama Plaintiffs and the Alabama Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Alabama Plaintiffs and the Alabama Subclass. Without the use of adequate data security, Alabama Plaintiffs and the Alabama Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

475. Plaintiffs and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT VII

Violation of AS 45.50.471, et seq. ("Unfair Trade Practices and Consumer Protection Act" (UTPCPA), On behalf of Alaska Plaintiffs and the Alaska Subclass against all Defendants

476. The Alaska Plaintiffs, individually and on behalf of the Alaska Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

477. Alaska's Unfair Trade Practices and Consumer Protection Act (UTPCPA) prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. AS 45.50.471.

478. Defendants violated the UTPCPA by engaging in conduct that constituted "unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce.

479. Specifically, Defendants collected and stored Plaintiffs' and the Alaska Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' and the Alaska Subclass's information, and failing to adequately segment the sensitive data from other parts of Change's servers and networks.

480. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible

without two-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of two factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

481. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes an immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Plaintiffs' and the Alaska subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Plaintiffs' and the Class's Personal Information. While Defendants profited off of Plaintiffs' and the Alaska Subclass's data, they failed to take the necessary measures to protect it, leaving Plaintiffs and the Class at significant and foreseeable risk of harm.

482. Although Defendants collectively acted in violation of the UTPCPA, each Defendant also separately violated the UTPCPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change, violated the UTPCPA by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Alaska subclass' Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own

policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

483. Optum also independently violated the UTPCPA. Upon its acquisition of Change Healthcare, Optum oversaw Change and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

484. Lastly, UHG also independently violated the UTPCPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient

information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

485. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

486. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Alaska Subclass at significant risk of harm.

487. Consequently, Defendants collectively and each independently took actions in violation of the UTPCPA.

488. As a result of those unlawful and unfair business practices, Plaintiffs and the Alaska Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

489. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

490. Alaska Plaintiffs and the Alaska Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because

Defendants continue to gather new medical information on Alaska Plaintiffs and the Alaska Subclass. Without the use of adequate data security, Alaska Plaintiffs and the Alaska Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

491. Alaska Plaintiffs and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT VIII

Violation of Protection of Personal Information Act, AS 45.48.010, *et seq*.

(On behalf of Alaska Plaintiffs and the Alaska Subclass against all Defendants)

492. Alaska Plaintiffs, individually and on behalf of the Alaska Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

493. "If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach." AS 45.48.010

494. Defendants are covered persons that own and/or license Personal Information within the meaning of AS 45.48.010 about Alaska Plaintiffs and the Alaska Subclass. Covered persons that own or license computerized data that includes Personal Information,

including Social Security numbers, medical information, and health information, are required to notify Alaska residents when a breach of the security of the information system that contains personal information occurs. Defendants are required to make the disclosure in the most expeditious time possible and without unreasonable delay. AS 45.48.010

495. Defendants became aware of the data breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024 that it had mailed notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

496. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform Plaintiffs and the Class as to whether they were impacted by the Data Breach. Because Plaintiffs and the Class had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, Plaintiffs and the Class could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that Plaintiffs could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical

provider or providers it obtained each individuals' medical information and, given that Change Healthcare could not make that determination, Plaintiffs lacked information to do so too.

497. Consequently, Plaintiffs and the Class did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which occurred at the earliest of five months after the breach and at the latest, over eight months later. That notice is insufficient under Alaska law.

498. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated AS 45.48.010.

499. As a direct and proximate result of Defendants' violations AS 45.48.010 Plaintiffs and Alaska Subclass Members suffered damages including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

500. Alaska Plaintiffs and Alaska Subclass Members seek relief under AS 45.48.010, including actual damages and injunctive relief.

COUNT IX

Violation of the Arizona Consumer Fraud Act, A.R.S. § 44-1521, et seq.

(On behalf of Arizona Plaintiffs and the Arizona Subclass against all Defendants)

501. Arizona Plaintiffs, individually and on behalf of the Arizona Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

502. Defendants sold Arizona Plaintiffs and other Arizona Subclass members "merchandise" as that term as defined by A.R.S. § 44-1521, in the form of services, including health and insurance services.

503. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A).

504. Defendants violated the Arizona Consumer Fraud Act by employing unfair acts and practices in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

505. Specifically, Defendants collected and stored Plaintiffs' and the Arizona Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Arizona Plaintiffs' and the Arizona Subclass's information, and failing to

adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

506. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, Optum Insight's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

507. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people, including Arizona Plaintiffs and the Arizona Subclass members. That is especially true because, despite failing to reasonably protect Arizona Plaintiffs' and the Arizona Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Arizona Plaintiffs' and the Arizona Subclass's Personal Information. While Defendants profited off of Arizona Plaintiffs' and the Arizona Subclass's data, they failed to take the necessary

measures to protect it, leaving Plaintiffs and the Class at significant and foreseeable risk of harm.

508. Although Defendants collectively acted in violation of the Arizona Consumer Fraud Act, each Defendant also separately violated the statute by acting unfairly, unlawfully, and unscrupulously. Specifically, following the merger between Change Healthcare and Optum Insight, they both violated the Act by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

509. Optum also independently violated the Arizona Consumer Fraud Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change

Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

510. Lastly, UHG also independently violated the Arizona Consumer Fraud Act. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

511. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

512. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount

of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Arizona Plaintiffs and Arizona Subclass members at significant risk of harm by failing to reasonably secure it.

513. Consequently, Defendants collectively and each independently took actions in violation of the Act.

514. As a result of those unlawful and unfair business practices, Arizona Plaintiffs and Arizona Subclass members' highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

515. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Arizona Plaintiffs and the Arizona Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the

misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

516. Arizona Plaintiffs and the Arizona Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Arizona Plaintiffs and the Arizona Subclass. Without the use of adequate data security, Arizona Plaintiffs and the Arizona Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

517. Arizona Plaintiffs and the Arizona Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and which the Court deems proper.

COUNT X

Violation of Cal. Bus. Code § 17200 ("UCL"), *et seq*.,

(On behalf of California Plaintiffs and the California Subclass against all Defendants)

518. The California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

519. California's Unfair Competition Law ("UCL") prohibits any person from committing an act of "unfair competition", including "any unlawful unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . . ." Cal. Civ. Code § 72000.

520. "[U]nfair competition" is interpreted broadly to include acts that violate other laws and may include acts even if not specifically proscribed by some other law.

521. Defendants violated the UCL by engaging in conduct that constituted "unlawful . . . business practices", including by violating the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

522. Specifically, Defendants collected and stored California Plaintiffs' and the California Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing California Plaintiffs' and California Subclass Members' Personal

Information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

523. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

524. Defendants' use of inadequate data security to protect servers containing large sums of highly sensitive Personal Information, including private medical information, were also unfair and unlawful because they violated other California statutes. Specifically, Defendants violated; (1) the California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of California Plaintiffs' and the California Subclass's Personal Information; and (2) the Consumer Records Act by failing to implement reasonable security to protect the Personal Information of California Plaintiffs and the California Subclass.

525. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to

over one hundred million people. That is especially true because, despite failing to reasonably protect California Plaintiffs' and California Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to California Plaintiffs' and the California Subclass's Personal Information. While Defendants profited off of California Plaintiffs' and the California Subclass's data, they failed to take the necessary measures to protect it, leaving Plaintiffs and the Class at significant and foreseeable risk of harm.

526. Although Defendants collectively acted in violation of the UCL, each Defendant also separately violated the UCL by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the UCL by developing the legacy server subject to the breach, including collecting and aggregating California Plaintiffs' and the California Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

527. Optum also independently violated the UCL. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation,

collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

528. Lastly, UHG also independently violated the UCL. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

529. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external

support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

530. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put California Plaintiffs and the California Subclass at significant risk of harm.

531. Consequently, Defendants collectively and each independently took actions in violation of the UCL.

532. As a result of those unlawful and unfair business practices, California Plaintiffs and the California Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen

information was posted on the dark web, exposing their Personal Information and putting patients at a substantial risk of misuse of their data.

533. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, California Plaintiffs and the California Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

534. California Plaintiffs and the California Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on California Plaintiffs and the California Subclass. Without the use of adequate data security, California Plaintiffs and the California Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

535. California Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional

and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and which the Court deems proper.

COUNT XI

Violation of the California Customer Records Act ("CCRA")
Cal. Civ. Code §§ 1798.80–.84

(On behalf of California Plaintiffs and the California Subclass against all Defendants)

536. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

537. "To ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains 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."

538. Defendants are a business enterprise that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about California Plaintiffs and the California Subclass. Businesses that own or license computerized data that includes Personal Information, including Social Security numbers, medical information, and health information, are required to notify California residents when their Personal Information has been acquired (or reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible without

unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

539. Defendants are a business enterprise that owns or licenses computerized data that includes Personal Information, as defined by Cal. Civ. Code § 1798.82.

540. California Plaintiffs and California Subclass Members' Personal Information includes the type of information covered by Cal. Civ. Code § 1798.82.

541. Because Defendants reasonably believed that California Plaintiffs' and the California Subclass's Personal Information was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach in "the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82.

542. By statute, Defendants were required to provide notice in a specific manner, using specific language and formatting under Cal. Civ. Code § 1798.82(d).

543. "The security breach notification shall be written in plain language, shall be titled 'Notice of Data Breach,' and shall present" certain required information "under the following headings: 'What Happened,' 'What Information Was Involved,' 'What We Are Doing,' 'What You Can Do,' and 'For More Information.'" Cal. Civ. Code § 1798.82(d)(1).

544. Defendants became aware of the data breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required

written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024, that they had mailed notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

545. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform California Plaintiffs and the California Subclass as to whether they were impacted by the Data Breach. Because California Plaintiffs and the California Subclass had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, California Plaintiffs and the California Subclass could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that California Plaintiffs and the California Subclass could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical provider or providers it obtained each individuals' medical information and, given that Change Healthcare could not make that determination, California Plaintiffs and the California Subclass lacked information to do so too.

546. Consequently, California Plaintiffs and the California Subclass did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which notice occurred, at the earliest, five months after the

breach and at the latest, over eight months later. That notice is insufficient under California law.

547. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

548. As a direct and proximate result of Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, California Plaintiffs and California Subclass Members suffered damages including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

549. California Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT XII

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

(On behalf of California Plaintiffs and the California Subclass against all Defendants)

550. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

551. Defendants are defined by statute as a healthcare provider subject to the CMIA because each had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of healthcare at the request of the individual or a provider of healthcare, for purposes of allowing the individual to manage the individual's information, or for the diagnosis and treatment of the individual[.]" Cal. Civ. Code § 56.06(a).

552. Defendants maintain medical information as defined by Cal. Civ. Code § 56.05 (j).

553. California Plaintiffs and California Subclass Members are patients, as defined in Cal. Civ. Code § 56.05(m). California Plaintiffs and California Subclass Members provided their personal medical information to Defendants through their medical providers.

554. At all relevant times, Defendants collected, stored, managed, and transmitted California Plaintiffs' and California Subclass Members' personal medical information.

555. Section 56.10(a) of the Cal. Civ. 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[.]"

556. As a result of the Data Breach, Defendants have misused, disclosed, and/or allowed third parties to access and view California Plaintiffs' and California Subclass Members' personal medical information without the written authorization that is required by Cal. Civ. Code § 56, et seq.

557. Various cybercriminals, including ALPHV, notchy, and RansomHub have accessed and obtained California Plaintiffs' and California Subclass Members' personal medical information, viewed it, and now have it available to sell to other bad actors or otherwise misuse.

558. As a further result of the Data Breach, the confidential nature of California Plaintiffs' and California Subclass Members' medical information was breached because of Defendants' negligence. Specifically, Defendants collected and stored California Plaintiffs' and the California Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing California Plaintiffs' and the California Subclass's Personal Information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks. Further, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to

prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

559. Defendants' misuse and/or disclosure of medical information regarding California Plaintiffs and California Subclass Members constitutes a violation of Cal. Civ. Code §§ 56.10, 56.11, 56.13, and 56.26.

560. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, California Plaintiffs' and California Subclass Members' personal medical information was accessed and disclosed without written authorization.

561. By disclosing California Plaintiffs' and California Subclass Members' Personal Information without their written authorization, Defendants violated Cal. Civ. Code § 56, et seq., and breached their legal duty to protect the confidentiality of such information, as well as Cal. Civ. Code §§ 56.06 and 56.101, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

562. 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 its violation of Cal. Civ. Code § 56, et seq., California Plaintiffs and California Subclass Members are entitled to (i) actual damages; (ii) punitive damages of up to $3,000 per Plaintiff and Class member; (iii) attorneys' fees up to $1,000; and (iv) litigation expenses and court costs under Cal. Civ. Code § 56.35.

COUNT XIII

Violation of the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code §§ 1798.100–.199.100

(On behalf of California Plaintiffs and the California Subclass against all Defendants)

563. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

564. California Plaintiffs and California Subclass Members are "consumer[s]" as defined by Cal. Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations."

565. Defendants are organized or operated for the profit or financial benefit of their shareholders. Defendants collected California Plaintiffs' and California Subclass Members' Personal Information as defined in Cal. Civ. Code § 1798.140.

566. Defendants are each a "business" as defined by Civ. Code § 1798.140(c), because Defendants:

a. are each 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";

b. "collect[] consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. do business in California; and

d. have annual gross revenues in excess of $25 million; annually buy, receive for the businesses' commercial purposes, sell or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derive 50 percent or more of their annual revenues from selling consumers' personal information.

567. Personal Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A), because it contains California Plaintiffs' and California Subclass Members' unencrypted first and last names, Social Security numbers, driver's license numbers, and/or medical information, among other information.

568. Defendants violated section 1798.150(a) of the California Consumer CCPA by failing to prevent California Plaintiffs' and California Subclass Members' nonencrypted and nonredacted Personal Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information of California Plaintiffs and California Subclass Members.

569. Specifically, Defendants collected and stored California Plaintiffs' and the California Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the

servers containing California Plaintiffs' and the California Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

570. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

571. Although Defendants collectively violated the CCPA by implementing unreasonable data security, each Defendant also separately violated the CCPA. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, developed and maintained the legacy server subject to the breach, including collecting and aggregating California Plaintiffs' and the California Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by

the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

572. Optum also independently violated the CCPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

573. Lastly, UHG also independently violated the CCPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

574. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

575. As a direct and proximate result of Defendants' misconduct, California Plaintiffs' and California Subclass Members' Personal Information was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendants' computer network.

576. As a direct and proximate result of Defendants' misconduct, California Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the loss of California Plaintiffs' and the California Subclass's legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as described above.

577. Based on Defendants' violations of the CCPA, California Plaintiffs and California Subclass Members have suffered actual pecuniary damages and seek to recover these damages along with any statutory or injunctive relief available under Cal. Civ. Code § 1798.150.

COUNT XIV

Violation of the Colorado Consumer Protection Act ("CoCPA")
Colo. Rev. Stat. §§ 6-1-101 to -116

(On behalf of Colorado Plaintiffs and the Colorado Subclass against all Defendants)

578. Colorado Plaintiffs, individually and on behalf of the Colorado Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

579. Colorado Plaintiffs have a right of action under the Colorado Consumer Protection Act pursuant to C.R.S. § 6-1-113.

580. The Colorado Consumer Protection Act prohibits "either knowingly or recklessly engag[ing] in any unfair, unconscionable, deceptive, deliberately misleading, false or fraudulent act or practice." C.R.S. § 6-1-105(1)(rrr).

581. Defendants violated the CoCPA by engaging in conduct unfair and unconscionable.

582. Specifically, Defendants collected and stored Colorado Plaintiffs' and Colorado Subclass Members' Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Colorado Plaintiffs' and the Colorado Subclass's Personal Information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

583. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory

requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

584. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Colorado Plaintiffs' and the Colorado Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Colorado Plaintiffs' and the Colorado Subclass's Personal Information. While Defendants profited off of Colorado Plaintiffs' and Colorado Subclass's data, they failed to take the necessary measures to protect it, leaving Colorado Plaintiffs and the Colorado Subclass at significant and foreseeable risk of harm.

585. Although Defendants collectively acted in violation of the CoCPA, each Defendant also separately violated the Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the CoCPA by

developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

586. Optum also independently violated the CoCPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

587. Lastly, UHG also independently violated the CoCPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring

Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

588. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

589. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to

adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Colorado Plaintiffs and the Colorado Subclass at significant risk of harm by failing to reasonably secure it.

590. Consequently, Defendants collectively and each independently took actions in violation of the CoCPA.

591. As a result of those unlawful and unfair business practices, Colorado Plaintiffs and Colorado Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

592. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Colorado Plaintiffs and the Colorado Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach;

and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

593. Colorado Plaintiffs and the Colorado Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Colorado Plaintiffs and the Colorado Subclass. Without the use of adequate data security, Colorado Plaintiffs and the Colorado Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

594. Colorado Plaintiffs and the Colorado Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XV

Violation of Connecticut Unfair Trade Practices Act ("CUTPA"), Conn. Gen. Stat. §§ 42-110a, *et seq*.

(On behalf of Connecticut Plaintiffs and the Connecticut Subclass against All Defendants)

595. Connecticut Plaintiffs, individually and on behalf of the Connecticut Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

596. CUTPA provides: "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

597. Each Connecticut Plaintiff and Connecticut Subclass member is a "person" as defined by Conn. Gen. Stat. § 42- 110a(3) and are consumers of Defendants' services and thus qualifies as a "person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b" under Conn. Gen. Stat. Ann. § 42-110g.

598. Each Defendant is a "person" as defined by Conn. Gen. Stat. Ann. § 42-110a(3).

599. Defendants advertised, offered, or sold goods or services in Connecticut and therefore engaged in trade or commerce directly or indirectly affecting the people of Connecticut. Conn. Gen. Stat. § 42-110a(4).

600. Unfair or deceptive acts or practices are those defined in CUTPA or by other Connecticut statutes, and are guided by the interpretation of the FTC Act.

601. The Connecticut data breach notification act, Conn. Gen. Stat. §36a701b, et seq., provides that failure to comply with the notice timelines constitutes an unfair and deceptive practice under CUTPA.

602. Specifically, Defendants collected and stored Connecticut Plaintiffs' and the Connecticut's Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the

data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Connecticut Plaintiffs' and the Connecticut Subclass's Personal Information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

603. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

604. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Connecticut Plaintiffs' and the Connecticut Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Connecticut Plaintiffs' and the Connecticut Subclass's Personal Information. While Defendants profited off of Connecticut Plaintiffs' and the

Connecticut Subclass's data, they failed to take the necessary measures to protect it, leaving Connecticut Plaintiffs and the Connecticut Subclass at significant and foreseeable risk of harm.

605. Although Defendants collectively acted in violation of CUTPA, each Defendant also separately violated the CUTPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the CUTPA by developing the legacy server subject to the breach, including collecting and aggregating Connecticut Plaintiffs' and the Connecticut Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

606. Optum also independently violated CUTPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control

over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

607. Lastly, UHG also independently violated CUTPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

608. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for responding to the Data Breach.

609. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change Healthcare), UHG failed to prioritize ensuring Change adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Subclass at significant risk of harm.

610. Consequently, Defendants collectively and each independently took actions in violation of CUTPA.

611. As a result of those unlawful and unfair business practices, Connecticut Plaintiffs' and the Connecticut Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

612. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity,

name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

613. Connecticut Plaintiffs and the Connecticut Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Connecticut Plaintiffs and the Connecticut Subclass. Without the use of adequate data security, Connecticut Plaintiffs and the Connecticut Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

614. Connecticut Plaintiffs and the Connecticut Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XVI

Violation of Ga. Code §§ 10-1-910, *et seq.*

(On behalf of Georgia Plaintiffs and the Georgia Subclass against All Defendants)

615. Georgia Plaintiffs, individually and on behalf of the Georgia Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

616. Georgia's Identity Theft Protection Act ("GITPA") requires "any information broker or data collector that maintains computerized data that includes personal information of individuals" to provide notice without unreasonable delay to Georgia residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Ga. Code § 10-11-912(a).

617. Defendants are businesses that own or license computerized data that includes Personal Information as defined by the GITPA.

618. Defendants therefore were required to disclose to Georgia Plaintiffs and Georgia Subclass members the existence of the Data Breach without unreasonable delay.

619. Defendants became aware of the Data Breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the Data Breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024, that it had mailed notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not

even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

620. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform Georgia Plaintiffs and the Georgia Subclass as to whether they were impacted by the Data Breach. Because Georgia Plaintiffs and the Georgia Subclass had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, Georgia Plaintiffs and the Georgia Subclass could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that Georgia Plaintiffs and the Georgia Subclass could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical provider or providers it obtained each individuals' medical information and, given that Change Healthcare could not make that determination, Georgia Plaintiffs and the Georgia Subclass lacked information to do so too.

621. Consequently, Georgia Plaintiffs and the Georgia Subclass did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which notice occurred, at the earliest, five months after the Data Breach and, at the latest, over eight months later. That notice is insufficient under Georgia law.

622. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated GITPA.

623. As a direct and proximate result of Defendants' violations of GITPA, Georgia Plaintiffs and Georgia Subclass members suffered and will continue to suffer damages including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

624. Georgia Plaintiffs and the Georgia Subclass seek all relief available at law, including monetary damages.

COUNT XVII

Violation of Hawaii Unfair or Deceptive Acts or Practices (UDAP), HI ST §480-1, *et seq*.

(On behalf of Hawaii Plaintiffs and the Hawaii Subclass against all Defendants)

625. The Hawaii Plaintiffs, individually and on behalf of the Hawaii Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

626. Hawaii's Unfair or Deceptive Acts or Practices (UDAP) prohibits any person from engaging in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. HI ST §480-2

627. The term "unfair or deceptive acts or practices" is to be interpreted broadly so as to stop and prevent fraudulent, unfair or deceptive business practices for the protection of both consumers and honest business[persons].

628. Defendants violated the UDAP by engaging in conduct that constituted "unfair or deceptive acts or practices", by collecting and storing Plaintiffs' and the Hawaii Subclass's Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' the Hawaii Subclass's information, and failing to adequately segment the sensitive data from other parts of Change's servers and networks.

629. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without two-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of two factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

630. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes an

immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Hawaii Plaintiffs' and the Hawaii Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Plaintiffs' and the Class's Personal Information. While Defendants profited off of Hawaii Plaintiffs' and the Hawaii Subclass's data, they failed to take the necessary measures to protect it, leaving Hawaii Plaintiffs and the Hawaii Subclass at significant and foreseeable risk of harm.

631. Although Defendants collectively acted in violation of the UDAP, each Defendant also separately violated the UDAP by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change, violated the UDAP by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Hawaii Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

632. Optum also independently violated the UDAP. Upon its acquisition of Change Healthcare, Optum oversaw Change and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

633. Lastly, UHG also independently violated the UDAP. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

634. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving

capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

635. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Hawaii Subclass at significant risk of harm.

636. Consequently, Defendants collectively and each independently took actions in violation of the UDAP.

637. As a result of those unlawful and unfair business practices, Plaintiffs and the Hawaii Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal

Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

638. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

639. Hawaii Plaintiffs and the Hawaii Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Hawaii Plaintiffs and the Hawaii Subclass. Without the use of adequate data security, Hawaii Plaintiffs and the Hawaii Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

640. Hawaii Plaintiffs and the Hawaii Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional

and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XVIII

Violation of Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505, *et seq.*

(On behalf of Illinois Plaintiffs and the Illinois Subclass against all Defendants)

641. Illinois Plaintiffs, individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

642. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") makes unlawful certain acts by persons in the conduct of trade or commerce. 815 Ill. Comp. Stat. § 505/2. Violating the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/1, *et seq*., is one such unlawful act. 815 Ill. Comp. Stat. 530/20.

643. The IPIPA requires "[a]ny data collector that owns or licenses personal information concerning an Illinois resident" to provide notice to the resident expediently and without unreasonable delay "that there has been a breach of the security of the system data following discovery or notification of the breach." 815 Ill. Comp. Stat. § 530/10.

644. Defendants are data collectors that own the personal information of Illinois's residents as defined by the IPIPA. 815 Ill. Comp. Stat. 530/5.

645. The IPIPA requires data collectors like Defendants that own or maintain "records that contain personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized

access, acquisition, destruction, use, modification, or disclosure." 815 Ill. Comp. Stat. § 530/45. Defendants failed to implement and maintain reasonable security measures as required by the statute.

646. Specifically, Defendants collected and stored Illinois Plaintiffs' and the Illinois Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Illinois Plaintiffs' and the Illinois Subclass's Personal Information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

647. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

648. Although Defendants collectively acted in violation of IPIPA, each Defendant also separately violated IPIPA. Specifically, Change Healthcare and Optum Insights, which merged after UHG's acquisition of Change Healthcare, violated IPIPA by

developing the legacy server subject to the breach, including collecting and aggregating Illinois Plaintiffs' and the Illinois Subclass's highly sensitive Personal Information and putting in place knowingly unreasonable data security to protect that information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

649. Optum also independently violated the IPIPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

650. Lastly, UHG also independently violated the IPIPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring

Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

651. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee[s]" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

652. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change Healthcare), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. population.

653. Consequently, Defendants collectively and each independently took actions in violation of the IPIPA. That is especially true because, despite failing to reasonably protect Illinois Plaintiffs' and the Illinois Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that Personal Information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Illinois Plaintiffs' and the Illinois Subclass's Personal Information. While Defendants profited off of Illinois Plaintiffs' and the Illinois Subclass's Personal Information, they failed to take the necessary measures to protect it, leaving Illinois Plaintiffs and the Illinois Subclass at significant and foreseeable risk of harm.

654. Illinois Plaintiffs and the Illinois Subclass's highly sensitive and private Personal Information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and Personal Information and putting patients at a substantial risk of misuse of their data.

655. Due to Defendants' inadequate security, the resulting Data Breach, and the unreasonably delayed notice, Illinois Plaintiffs and the Illinois Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the

access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

656. Illinois Plaintiffs and the Illinois Subclass also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Illinois Plaintiffs and the Illinois Subclass. Without the use of adequate data security, Illinois Plaintiffs and the Illinois Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

657. Illinois Plaintiffs and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XIX

Violation of the Louisiana Database Security Breach Notification Law, La. R.S. 51:3701, et seq.

(On behalf of Louisiana Plaintiffs and the Louisiana Subclass against all Defendants)

658. Louisiana Plaintiffs, individually and on behalf of the Louisiana Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

659. The Louisiana Database Security Breach Notification Law provides that "[a]ny person that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person." La. R.S. 51:3704(C).

660. Defendants are persons that own maintain, and license Personal Information, within the meaning of La. R.S. 51:3704, about Louisiana Plaintiffs and the Louisiana Subclass. Businesses that own or license computerized data that includes Personal Information, including Social Security numbers, medical information, and health information, are required to notify Louisiana residents when their Personal Information has been acquired (or reasonably believed to have been acquired) "in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach" La. R.S. 51:3704E.

661. Louisiana Plaintiffs' and Louisiana Subclass Members' Personal Information includes the type of information covered by La. R.S. 51:3704.

662. Defendants became aware of the data breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024 that it had mailed

notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

663. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform Plaintiffs and the Class as to whether they were impacted by the Data Breach. Because Plaintiffs and the Class had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, Plaintiffs and the Class could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that Plaintiffs could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical provider or providers it obtained each individuals' medical information and, given that Change Healthcare could not make that determination, Plaintiffs lacked information to do so too.

664. Consequently, Plaintiffs and the Class did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which occurred at the earliest of five months after the breach and at the latest, over eight months later. That notice is insufficient under Louisiana law.

665. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated La. R.S. 3704.

666. As a direct and proximate result of Defendants' violations La. R.S. 51:3704 Louisiana Plaintiffs and Louisiana Subclass Members suffered damages including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

667. Louisiana Plaintiffs and Louisiana Subclass Members seek relief under La. R.S. 51:3705, including actual damages and injunctive relief.

COUNT XX

Violation of Louisiana Unfair Trade Practices Act (LUPTA), LA RS 51 §1405, *et seq*.

(On behalf of Louisiana Plaintiffs and the Louisiana Subclass against all Defendants)

668. The Louisiana Plaintiffs, individually and on behalf of the Louisiana Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

669. Louisiana's Unfair Trade Practices Act (LUPTA) prohibits any person from engaging in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. La. R.S. 51:1405 (A).

670. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, 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. La. R.S. 51:3704 (A).

671. Violation of the provisions of La. R.S. 51:3704 (A) shall constitute an unfair act or practice under La. R.S. 51:1405(A).

672. Defendants violated LUPTA by engaging in conduct that constituted "unfair or deceptive acts or practices", by collecting and storing Plaintiffs' and the Louisiana Subclass's Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' the Louisiana Subclass's information, and failing to adequately segment the sensitive data from other parts of Change's servers and networks.

673. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and

Change Healthcare's own policies, access to the breached legacy database was possible without two-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of two factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

674. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes an immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Louisiana Plaintiffs' and the Louisiana Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Louisiana Plaintiffs' and the Louisiana Subclass's Personal Information. While Defendants profited off of Louisiana Plaintiffs' and the Louisiana Subclass's data, they failed to take the necessary measures to protect it, leaving Louisiana Plaintiffs and the Louisiana Subclass at significant and foreseeable risk of harm.

675. Although Defendants collectively acted in violation of LUPTA, each Defendant also separately violated the LUPTA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change, violated LUPTA by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the

Louisiana Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

676. Optum also independently violated LUPTA. Upon its acquisition of Change Healthcare, Optum oversaw Change and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

677. Lastly, UHG also independently violated LUPTA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and

modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

678. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

679. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to

adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Louisiana Subclass at significant risk of harm.

680. Consequently, Defendants collectively and each independently took actions in violation of LUPTA.

681. As a result of those unlawful and unfair business practices, Plaintiffs and the Louisiana Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

682. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

683. Louisiana Plaintiffs and the Louisiana Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Louisiana Plaintiffs and the Louisiana Subclass. Without the use of adequate data security, Louisiana Plaintiffs and the Louisiana Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

684. Louisiana Plaintiffs and the Louisiana Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper pursuant to La. R.S. 51:1409.

COUNT XXI

Violation of the Maine Unfair Trade Practices Act, 5 M.R.S. § 205-A, *et seq*.

(On behalf of Maine Plaintiffs and the Maine Subclass against all Defendants)

685. Maine Plaintiffs, individually and on behalf of the Maine Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

686. Maine's Unfair Trade Practices Act prohibits any person from committing acts of "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" 5 M.R.S. § 206. The Maine Unfair Trade Practices Act expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. *See* 5 M.R.S. § 207(1).

687. Maine Plaintiffs and Maine Subclass members are each a "person" as defined by 5 M.R.S. § 206(2). Maine Plaintiffs and Maine Subclass members are also each a "person" as defined by 5 M.R.S. § 213(1) as each purchased goods and/or services primarily for personal, family, and/or household purposes and suffered and will continue to suffer a "loss of money or property, real or personal, as a result of the use or employment by [Defendants] of a method, act or practice declared unlawful by" this statute. Indeed, Maine Plaintiffs and the Maine Subclass paid for insurance for personal and family medical health expenses, and further, provided their data to Change Healthcare indirectly via their medical providers upon obtaining personal medical treatment. Their personal information, which constitutes personal property of significant value (as evidenced by the substantial benefit Defendants received from its use), has been diminished by its disclosure to cybercriminals because it has lost valuable features, including confidentiality and privacy.

688. "[U]nfair methods of competition" is interpreted broadly to include acts that violate other laws and may include acts even if not specifically proscribed by some other law.

689. Defendants are each a "person" as defined by 5 M.R.S. § 206(2).

690. Defendants' conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 M.R.S. § 206(3).

691. Defendants violated Maine's Unfair Trade Practices Act by engaging in conduct that constituted unfair trade acts and practices in the conduct of trade or commerce, in violation of 5 M.R.S. § 207.

692. Specifically, Defendants collected and stored Maine Plaintiffs' and the Maine's Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Maine Plaintiffs' and the Maine Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

693. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

694. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people, including Maine Plaintiffs and Maine Subclass members.

695. Although Defendants collectively acted in violation of Maine's Unfair Trade Practices Act, each Defendant also separately violated Maine's Unfair Trade Practices Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated the Maine's Unfair Trade Practices Act by developing the legacy server subject to the breach, including collecting and aggregating Maine Plaintiffs' and the Maine Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

696. Optum also independently violated the Maine Unfair Trade Practices Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure

to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

697. Lastly, UHG also independently violated Maine's Unfair Trade Practices Act. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change was required to implement.

698. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee[s]" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for responding to and investigating the Data Breach.

699. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount

of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. population. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Maine Plaintiffs and the Maine Subclass at significant risk of harm.

700. Consequently, Defendants collectively and each independently took actions in violation of Maine's Unfair Trade Practices Act.

701. As a result of those unlawful and unfair business practices, Maine Plaintiffs and the Maine Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

702. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Maine Plaintiffs and the Maine Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal

Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

703. Maine Plaintiffs and the Maine Subclass also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Maine Plaintiffs and the Maine Subclass. Without the use of adequate data security, Maine Plaintiffs and the Maine Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

704. Defendants previously received notice of potential state statutory claims more than thirty days before the filing of the Complaint. Defendants' counsel informed Plaintiffs' counsel that it was on notice of the potential state statutory claims and would not respond to any subsequent notice. Consequently, Defendants waived any further notice requirement.

705. Maine Plaintiffs and the Maine Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law;

court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXII

Violation of Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, *et seq*.

(On behalf of Maryland Plaintiffs and the Maryland Subclass against all Defendants)

706. Maryland Plaintiffs, individually and on behalf of the Maryland Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

707. The Maryland Consumer Protection Act ("Maryland CPA") provides that a person may not engage in any unfair, abusive, or deceptive trade practice, including: "[f]alse, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers"; "[f]ailure to state a material fact if the failure deceives or tends to deceive"; and "[d]eception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same." Md. Code Ann., Com. Law § 13-301. The statute further provides that a person may not engage in such conduct regardless of whether the consumer is actually deceived or damaged. Md. Code Ann., Com. Law § 13-302. The statute expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. *See* Md. Code Ann., Com. Law § 13-105.

708. The Maryland CPA also provides that violation of the Social Security Number Privacy Act, Md. Code Ann., Comm. Law, § 14-3401, *et seq*., constitutes an unfair, abusive, or deceptive practice under the Maryland CPA. Md. Code Ann., Com.

Law § 13-301(14)(xxi). As alleged herein, Defendants violated the Social Security Number Privacy Act and therefore committed a violation of the Maryland CPA.

709. A violation of the Maryland Personal Information Privacy Act, Md. Code Ann., Com. Law § 14-3501, *et seq*., also "[i]s an unfair or deceptive trade practice within the meaning of" the Maryland CPA. Md. Code Ann., Com. Law § 14-3508(1). As alleged herein, Defendants violated the Personal Information Privacy Act and therefore committed a violation of the Maryland CPA.

710. Maryland Plaintiffs and Maryland Subclass members are "consumers" as defined by Md. Code Ann., Comm. Code § 13-101(c).

711. Defendants are each a "person" within the meaning of Md. Code Ann., Com. Law § 13-101(h).

712. Defendants advertise, offer, or sell "consumer goods" or "consumer services" as defined by Md. Code Ann., Comm. Code § 13-101(d).

713. Defendants violated the Maryland CPA by engaging in unfair, abusive, or deceptive trade practices, in violation of Md. Code Ann., Comm. Code § 13-301. The Maryland CPA provides that a person may not engage in any unfair, abusive, or deceptive trade practice in the sale of any consumer good or consumer services. Md. Code Ann., Comm. Code §13-303. Defendants participated in unfair, abusive, or deceptive acts that violated the Maryland CPA.

714. Specifically, Defendants collected and stored Maryland Plaintiffs' and the Maryland Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of

data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Maryland Plaintiffs' and the Maryland Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

715. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

716. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people, including Maryland Plaintiffs and the Maryland Subclass. That is especially true because, despite failing to reasonably protect Maryland Plaintiffs' and the Maryland Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Maryland Plaintiffs'

and the Maryland Subclass's Personal Information. While Defendants profited off of Maryland Plaintiffs' and the Maryland Subclass's data, they failed to take the necessary measures to protect it, leaving Maryland Plaintiffs and the Maryland Subclass at significant and foreseeable risk of harm.

717. Although Defendants collectively acted in violation of the Maryland CPA, each Defendant also separately violated the Maryland CPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated the Maryland CPA by developing the legacy server subject to the Data Breach, including collecting and aggregating Maryland Plaintiffs' and the Maryland Subclass's highly sensitive Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

718. Optum also independently violated the Maryland CPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to

Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

719. Lastly, UHG also independently violated the Maryland CPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

720. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee[s]" "risk management" and "cybersecurity" and that its Audit and Finance

Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

721. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change Healthcare), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. population.

722. Consequently, Defendants collectively and each independently took actions in violation of the Maryland CPA.

723. As a result of those unlawful and unfair business practices, Maryland Plaintiffs and the Maryland Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

724. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Maryland Plaintiffs and the Maryland Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2)

misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

725. Maryland Plaintiffs and the Maryland Subclass also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Maryland Plaintiffs and the Maryland Subclass. Without the use of adequate data security, Maryland Plaintiffs and the Maryland Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

726. Maryland Plaintiffs and the Maryland Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXIII

Violation of Massachusetts Consumer Protection Act,
Mass. Gen. Laws Ann. Ch. 93A § 1, et seq.

(On behalf of Massachusetts Plaintiffs and the Massachusetts Subclass against all Defendants)

727. Massachusetts Plaintiffs, individually and on behalf of the Massachusetts Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

728. Chapter 93A of the Massachusetts Consumer Protection Act forbids "unfair or deceptive acts or practices in the conduct of any trade or commerce." Mass. Gen. Laws ch. 93A, § 2(a). Chapter 93A expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. Mass. Gen. Laws ch. 93A, § 2(b).

729. Massachusetts Plaintiffs and members of the Massachusetts Subclass are each a "person" as defined by the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §1(a) and, as alleged herein, have "been injured by another person's use or employment of any method, act or practice declared to be unlawful" under Ch. 93A. Mass. Gen. Laws Ann. ch. 93A, § 9.

730. Defendants are each a "person" as defined by the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §1(a).

731. Defendants engaged in "trade" or "commerce" defined as advertising, the offering for sale, rent or lease, the sale, rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security and any contract of

sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situated. Mass. Gen. Laws Ann. Ch. 93A, §1(b).

732. Defendants engaged in trade or commerce that directly or indirectly affects the people of the Commonwealth of Massachusetts

733. Specifically, Defendants collected and stored Massachusetts Plaintiffs' and the Massachusetts Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Massachusetts Plaintiffs' and the Massachusetts Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers networks.

734. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

735. Defendants had a duty to keep the Personal Information safe and secure under HIPAA and regulations promulgated thereunder, the FTCA and regulations promulgated thereunder, and Mass. Gen. Laws Ch. 93H, §2 and regulations promulgated thereunder.

736. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Massachusetts Plaintiffs' and the Massachusetts Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Massachusetts Plaintiffs' and the Massachusetts Subclass's Personal Information. While Defendants profited off of Massachusetts Plaintiffs' and the Massachusetts Subclass's data, they failed to take the necessary measures to protect it, leaving Plaintiffs and the Class at significant and foreseeable risk of harm.

737. Although Defendants collectively acted in violation of the Massachusetts Consumer Protection Act, each Defendant also separately violated the Massachusetts Consumer Protection Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged with Change Healthcare after UHG's acquisition, violated the Massachusetts Consumer Protection Act by developing the legacy server subject to the breach, including collecting and aggregating Massachusetts

Plaintiffs' and the Massachusetts Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

738. Optum also independently violated the Massachusetts Consumer Protection Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

739. Lastly, UHG also independently violated the Massachusetts Consumer Protection Act. UHG controlled and oversaw Change Healthcare generally, and its

cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

740. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for responding to the Data Breach.

741. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change Healthcare), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps,

including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S.

742. Consequently, Defendants collectively and each independently took actions in violation of the Massachusetts Consumer Protection Act.

743. Defendants' unfair or deceptive acts and practices complained of herein affected the public interest and consumers at large, including Massachusetts Plaintiffs and the Massachusetts Subclass, who are Massachusetts residents affected by the Data Breach. Massachusetts Plaintiffs and the Massachusetts Subclass each were injured in Massachusetts.

744. As a result of those unlawful and unfair business practices, Massachusetts Plaintiffs and the Massachusetts Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

745. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6)

emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

746. Defendants previously received notice of potential state statutory claims more than thirty days before the filing of the Complaint. Defendants' counsel informed Plaintiffs' counsel that it was on notice of the potential state statutory claims and would not respond to any subsequent notice. Consequently, Defendants waived any further notice requirement.

747. Massachusetts Plaintiffs and the Massachusetts Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXIV

Violation of the Minnesota Deceptive Trade Practices Act ("MDTPA"), Minn. Stat. § 325D.43

(On Behalf of Plaintiffs and the Nationwide Subclass)

748. Minnesota Plaintiffs, individually and on behalf of the Nationwide Class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

749. Minnesota affords a cause of action to any person harmed by an entities use of deceptive trade practices. Minn. Stat. § 325D.45, Subd.3.

750. Under MDTPA, a "person engages in a deceptive trade practice when, in the course of business, vocation or occupation, the person . . . engaged in (i) unfair methods of competition, or (ii) unfair or unconscionable acts or practices[.]". Minn. Stat. § 325D.44, subd. 1(13).

751. Defendants engaged in conduct that violated the MDTPA.

752. Specifically, Defendants collected and stored Plaintiffs' and the Minnesota Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' and the Class's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

753. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

754. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change

Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over a hundred million people. That is especially true because, despite failing to reasonably protect Minnesota Plaintiffs' and the Minnesota Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Minnesota Plaintiffs' and the Minnesota Subclass's Personal Information. While Defendants profited off of Minnesota Plaintiffs' and the Minnesota Subclass's data, they failed to take the necessary measures to protect it, leaving Minnesota Plaintiffs and the Minnesota Subclass at significant and foreseeable risk of harm.

755. Although Defendants collectively acted in violation of MDTPA, each Defendant also separately violated the statute by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged upon UHG's acquisition of Change Healthcare, violated the MDTPA by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

756. Optum also independently violated the MDTPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

757. Lastly, UHG also independently violated the MDTPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

758. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving

capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

759. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Plaintiffs and the Subclass at significant risk of harm by failing to reasonably secure it.

760. As a result of those unlawful and unfair business practices, Plaintiffs and the Minnesota Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was

posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

761. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

762. Minnesota Plaintiffs and the Minnesota Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Minnesota Plaintiffs and the Minnesota Subclass. Without the use of adequate data security, Minnesota Plaintiffs and the Minnesota Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

763. Minnesota Plaintiffs and the Minnesota Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the

law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXV

Violation of the Minnesota Health Records Act Minn. Stat. §§ 144.291 and 144.293

(On Behalf of the Plaintiffs and the Nationwide Class)

764. Plaintiffs, individually and on behalf of the Class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

765. Under the Minnesota Health Records Act, "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment for the provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c) (the "MHRA").

766. The Personal Information of Plaintiffs and the Class that was released in the Data Breach involved health records as that term is defined in the MHRA.

767. Plaintiffs and the Class are "patients" as that term is defined under the MHRA at all times relevant to this action under Minn. Stat. § 144.291, subd. 2(g).

768. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

769. Via the Data Breach, Defendants released Plaintiffs' and the Class's health records, which were actually accessed, viewed, and obtained by cybercriminals.

770. Neither Plaintiffs nor the Class consented to have their health records released in the Data Breach.

771. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees. Minn. Stat. § 144.298, subd. 2. As a result of Defendants' violations of the MHRA, Plaintiffs and the other Class members seek all damages authorized by law, including compensatory damages plus costs, and reasonable attorney fees.

COUNT XXVI

Violation of New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:1 et seq.,

(On behalf of New Hampshire Plaintiffs and the New Hampshire Subclass against all Defendants)

772. New Hampshire Plaintiffs, individually and on behalf of the New Hampshire Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

773. The New Hampshire Consumer Protection Act ("NHCPA") prohibits a person or entity from using "any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." An unfair practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers, offends public policy as established by law or by other established concepts of unfairness,

and is of the type proscribed by the NHCPA, attaining the level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce. The statute expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act.

774. New Hampshire Plaintiffs and members of the New Hampshire Subclass are each a "person" under the NHCPA. N.H. Rev. Stat. §358-A:1(I). As alleged herein, New Hampshire Plaintiffs and members of the New Hampshire Subclass each were "injured by another's use of any method, act or practice declared unlawful under this chapter." N.H. Rev. Stat. Ann. § 358-A:10(I).

775. Defendants are each a "person" under the NHCPA. N.H. Rev. Stat. §358-A:1(I).

776. The New Hampshire statutory scheme provides a non-exhaustive list of acts that constitute violations of the statute.

777. The New Hampshire Supreme Court has held that conduct that is not specifically delineated within the statutory scheme is analyzed under the "rascality test." *Axenics, Inc. v. Turner Constr. Co*., 62 A.3d 754, 768-69 (N.H. 2013).

778. Defendants engaged in the conduct alleged in this complaint through transactions in and involving trade and commerce within the State of New Hampshire. N.H. Rev. Stat. §358A:2.

779. While involved in trade or commerce, Defendants violated the NHCPA by engaging in unfair, deceptive, and unconscionable business practices.

780. Specifically, Defendants collected and stored New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing New Hampshire Plaintiffs' and the New Hampshire Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

781. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

782. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect New Hampshire Plaintiffs' and the New Hampshire Subclass's highly

sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information. While Defendants profited off of New Hampshire Plaintiffs' and the New Hampshire Subclass's data, they failed to take the necessary measures to protect it, leaving New Hampshire Plaintiffs and the New Hampshire Subclass at significant and foreseeable risk of harm.

783. Although Defendants collectively acted in violation of the NHCPA, each Defendant also separately violated the NHCPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following the acquisition of Change Healthcare, violated the NHCPA by developing the legacy server subject to the breach, including collecting and aggregating New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

784. Optum also independently violated the NHCPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed

under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

785. Lastly, UHG also independently violated the NHCPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

786. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors

"oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

787. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S.

788. Consequently, Defendants collectively and each independently took actions in violation of the NHCPA.

789. Defendants' unfair or deceptive acts and practices complained of herein affected the public interest and consumers at large, including New Hampshire Plaintiff and the New Hampshire Subclass, who are New Hampshire residents affected by the Data Breach. New Hampshire Plaintiffs and the New Hampshire Subclass each were injured in New Hampshire.

790. As a result of those unlawful and unfair business practices, New Hampshire Plaintiffs' and the New Hampshire's Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and

successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

791. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

792. New Hampshire Plaintiffs and the New Hampshire Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on New Hampshire Plaintiffs and the New Hampshire Subclass. Without the use of adequate data security, New Hampshire Plaintiffs and the New Hampshire Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

793. New Hampshire Plaintiffs and the New Hampshire Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXVII

Violation of the New Hampshire Right to Privacy Statute, N.H. Rev. Stat. § 359-C:19, et seq.,

(On behalf of New Hampshire Plaintiffs and the New Hampshire Subclass against all Defendants)

794. New Hampshire Plaintiffs, individually and on behalf of the New Hampshire Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

795. The New Hampshire Right to Privacy Statute requires that any person doing business in New Hampshire who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If a determination is made that the information has been misused or is reasonably likely to be misused, the person shall notify the affected individuals as soon as possible.

796. Defendants are each a "person" for purposes of RSA § 359 who own or license computerized data that includes personal information.

797. Defendants violated RSA § 359-C:20 by failing to promptly determine whether personal information within its control has been or will be misused and by failing to promptly notify affected individuals of such harm or risk of harm.

798. Pursuant to under RSA § 359-C:20(VI)(a), Defendants were required to notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the anticipated date of the notification to consumers, the approximate number of consumers who will be notified, and the content of the notice.

799. As alleged herein, Defendants did not comply with their consumer reporting agency reporting requirements of notifying affected individuals without unreasonable delay. As a direct and proximate result, New Hampshire Plaintiffs and the New Hampshire Subclass members suffered injuries and will continue to suffer injuries, as described herein.

800. Defendants' unreasonable delay in complying with its notification obligations was willful and knowing.

801. Specifically, Defendants collected and stored New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing New Hampshire Plaintiffs' and the New Hampshire Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

802. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

803. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect New Hampshire Plaintiffs' and the New Hampshire Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information. While Defendants profited off of New Hampshire Plaintiffs' and the New Hampshire Subclass's data, they failed to take the necessary measures to protect it, leaving New Hampshire Plaintiffs and the New Hampshire Subclass at significant and foreseeable risk of harm.

804. Although Defendants collectively acted in violation of the New Hampshire Right to Privacy Statute, each Defendant also separately violated the New Hampshire Right to Privacy Statute by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged after the acquisition of Change Healthcare, violated the New Hampshire Right to Privacy Statute by developing the legacy server subject to the breach, including collecting and aggregating New Hampshire Plaintiffs' and the New Hampshire Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

805. Optum also independently violated the New Hampshire Right to Privacy Statute. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal

Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

806. Lastly, UHG also independently violated the New Hampshire Right to Privacy Statute. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

807. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

808. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S.

809. Consequently, Defendants collectively and each independently took actions in violation of the New Hampshire Right to Privacy Statute.

810. As a result of those unlawful and unfair business practices, New Hampshire Plaintiffs and the New Hampshire Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

811. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of

security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

812. New Hampshire Plaintiffs and the New Hampshire Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on New Hampshire Plaintiffs and the New Hampshire Subclass. Without the use of adequate data security, New Hampshire Plaintiffs and the New Hampshire Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

813. New Hampshire Plaintiffs and the New Hampshire Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXVIII

Violation of N.J. Stat. § 56:8-1, *et seq.*

(On behalf of New Jersey Plaintiffs and the New Jersey Subclass against all Defendants)

814. New Jersey Plaintiffs, individually and on behalf of the New Jersey Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

815. The New Jersey Consumer Fraud Act ("NJCFA") makes unlawful certain acts by persons in any commercial practice. N.J. Stat. § 56:8-2. Violating New Jersey's data-breach notice statute is an unlawful practice under the NJCFA. N.J. Stat. § 56:8-160.

816. The notice statute requires "any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information" to provide notice without unreasonable delay to New Jersey residents "whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person." N.J. Stat. § 56:8-163(a).

817. Defendants are businesses that compile and maintain computerized records that contain personal information as defined in N.J. Stat. § 56:8-161.

818. Defendants therefore were required to disclose to New Jersey Plaintiffs and New Jersey Subclass members the existence of the Data Breach without unreasonable delay.

819. Defendants became aware of the Data Breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required

written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024, that it had mailed notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

820. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform Plaintiffs and the Class as to whether they were impacted by the Data Breach. Because Plaintiffs and the Class had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, Plaintiffs and the Class could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that Plaintiffs could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical provider or providers it obtained each individual's medical information and, given that Change Healthcare could not make that determination, Plaintiffs lacked information to do so too.

821. Consequently, Plaintiffs and the Class did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which occurred at the earliest of five months after the breach and at the latest, over eight months later. That notice is insufficient under New Jersey law.

822. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

823. New Jersey Plaintiffs and the New Jersey Subclass seek all relief available by law including monetary damages and injunctive relief.

COUNT XXIX

Violation of the New Mexico Unfair Practices Act- NM Stat. § 57-12-10, *et seq*.,

(On behalf of New Mexico Plaintiffs and the New Mexico Subclass against all Defendants)

824. New Mexico Plaintiffs, individually and on behalf of the New Mexico Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

825. Defendants are each a "person" as meant by N. M. Stat. § 57-12-2.

826. Defendants were engaged in "trade" and "commerce" as meant by N.M. Stat.§ 57-12-2(C) when performing their various functions and operating EDI

Clearinghouses, processing medical transactions, and the collection, maintenance and storage of New Mexico Plaintiffs' and New Mexico Subclass Members' Personal Information as part of the functions each Defendant serves within the healthcare industry.

827. The New Mexico Unfair Practices Act, N. M. Stat. § 57-12-2, *et seq*., prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

828. Defendants violated the New Mexico Unfair Practices Act ("Act") by engaging in unfair conduct.

829. Specifically, Defendants collected and stored New Mexico Plaintiffs' and the New Mexico Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing New Mexico Plaintiffs' and the New Mexico Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

830. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of

multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

831. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect New Mexico Plaintiffs' and the New Mexico Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to New Mexico Plaintiffs' and the New Mexico Subclass's Personal Information. While Defendants profited off of New Mexico Plaintiffs' and the New Mexico Subclass's data, they failed to take the necessary measures to protect it, leaving New Mexico Plaintiffs and the New Mexico Subclass at significant and foreseeable risk of harm.

832. Although Defendants collectively acted in violation of the Act, each Defendant also separately violated the Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the Act by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed

to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

833. Optum also independently violated the Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident–response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

834. Lastly, UHG also independently violated the Act. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient

information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

835. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

836. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change Healthcare), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put New Mexico Plaintiffs and the New Mexico Subclass at significant risk of harm by failing to reasonably secure it.

837. Consequently, Defendants, collectively, and each, independently, took actions in violation of the Act.

838. As a result of those unlawful and unfair business practices, New Mexico Plaintiffs and the New Mexico Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

839. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

840. New Mexico Plaintiffs and the New Mexico Subclass also remain at heightened risk of future injury because their information resides with Defendants and,

further, because Defendants continue to gather new medical information on New Mexico Plaintiffs and the New Mexico Subclass. Without the use of adequate data security, New Mexico Plaintiffs and the New Mexico Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

841. New Mexico Plaintiffs and the New Mexico Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXX

Violation of N.Y. Gen. Bus. Law § 349

(On behalf of New York Plaintiffs and the New York Subclass against all Defendants)

842. New York Plaintiffs, individually and on behalf of the New York Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

843. New York General Business Law §349(a) states, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." New York courts specifically interpret § 349 "by looking to the definition of deceptive acts and practices under [S]ection 5 of the Federal Trade Commission Act." *New York v. Feldman*, 210 F. Supp. 2d 294, 302 (S.D.N.Y. 2002).

844. Defendants are each a "person, firm, corporation or association or agent or employee thereof" within the meaning of N.Y. Gen. Bus. Law § 349(b).

845. At all relevant times, Defendants were engaged in "business," "trade," or "commerce" within the meaning of N.Y. Gen. Bus. Law § 349(a).

846. New York Plaintiffs and New York Subclass members are each a "person" within the meaning of N.Y. Gen. Bus. Law § 349(h).

847. At all relevant times, Defendants engaged in transactions affecting trade or commerce and furnishing services in New York including, but not limited to, the responsibility for overseeing or contributing to the protocols for properly safeguarding New York Plaintiffs' and New York Subclass members' Personal Information.

848. Specifically, Defendants collected and stored New York Plaintiffs' and the New York Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing New York Plaintiffs' and New York Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

849. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of

multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

850. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect New York Plaintiffs and New York Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

851. New York Plaintiffs and members of the New York Subclass were deceived in New York. They also transacted with Defendants in New York by providing their Personal Information for medical care and treatment in New York.

852. Defendants' deceptive conduct is material because it was likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

853. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect New York Plaintiffs' and the New York Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to New York Plaintiffs' and the New York Subclass's Personal Information. While Defendants profited off of New York Plaintiffs' and the New York Subclass's data, they failed to take the necessary measures to protect it, leaving New York Plaintiffs and the New York Subclass at significant and foreseeable risk of harm.

854. Although Defendants collectively acted in violation of N.Y. Gen. Bus. Law § 349, each Defendant also separately violated N.Y. Gen. Bus. Law § 349 by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated N.Y. Gen. Bus. Law § 349 by developing the legacy server subject to the breach, including collecting and aggregating New York Plaintiffs' and the New York Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that

Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

855. Optum also independently violated N.Y. Gen. Bus. Law § 349. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

856. Lastly, UHG also independently violated N.Y. Gen. Bus. Law § 349. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the

patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

857. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

858. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put New York Plaintiffs and New York Subclass members at significant risk of harm.

859. Consequently, Defendants, collectively, and each, independently, took actions in violation of N.Y. Gen. Bus. Law § 349.

860. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

861. As a result of those unlawful and unfair business practices, New York Plaintiffs' and the New York Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

862. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, the above deceptive and unlawful practices and acts by Defendants caused and will continue to cause substantial injuries to New York Plaintiffs and New York Subclass members that they could not reasonably avoid, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions;

(9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

863. New York Plaintiffs and the New York Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonably necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXI

Violation of North Carolina Unfair and Deceptive Trade Practices Act,

N.C. Gen. Stat. § 75.1.1, *et seq*.,

(On behalf of North Carolina Plaintiffs and the North Carolina Subclass against all Defendants)

864. North Carolina Plaintiffs, individually and on behalf of the North Carolina Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

865. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." N.C. Gen. Stat. Ann. § 75-1.1.

866. "[U]nfair methods of competition" is interpreted broadly to include acts that violate other laws and may include acts even if not specifically proscribed by some other law.

867. Defendants advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b)

868. Specifically, Defendants collected and stored North Carolina Plaintiffs' and the North Carolina Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing North Carolina Plaintiffs' and the North Carolina Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

869. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

870. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes

immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect North Carolina Plaintiffs' and the North Carolina Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to North Carolina Plaintiffs' and the North Carolina Subclass's Personal Information. While Defendants profited off of North Carolina Plaintiffs' and the North Carolina Subclass's data, they failed to take the necessary measures to protect it, leaving North Carolina Plaintiffs and the North Carolina Subclass at significant and foreseeable risk of harm.

871. Although Defendants collectively acted in violation of the NCUDTPA, each Defendant also separately violated the NCUDTPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated the NCUDTPA by developing the legacy server subject to the breach, including collecting and aggregating North Carolina Plaintiffs' and the North Carolina Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

872. Optum also independently violated the NCUDTPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored, were unfair and unlawful acts.

873. Lastly, UHG also independently violated the NCUDTPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

874. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

875. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put North Carolina Plaintiffs and the North Carolina Subclass at significant risk of harm.

876. Consequently, Defendants, collectively, and each, independently, took actions in violation of the NCUDTPA.

877. As a result of those unlawful and unfair business practices, North Carolina Plaintiffs and the North Carolina Subclass's highly sensitive and private health and medical

information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

878. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

879. North Carolina Plaintiffs and the North Carolina Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on North Carolina Plaintiffs and the North Carolina Subclass. Without the use of adequate data security, North Carolina Plaintiffs and the North Carolina Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

880. North Carolina Plaintiffs and the North Carolina Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXII

Violation of North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq*.,

(On behalf of North Carolina Plaintiffs and the North Carolina Subclass against all Defendants)

881. North Carolina Plaintiffs, individually and on behalf of the North Carolina Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

882. In pertinent part, N.C. Gen. Stat. § 75-65 provides:

> Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

883. N.C. Gen. Stat. § 14-113.20b defines "Personal Information" as a person's first name or initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State:

a. Social security or employer taxpayer identification numbers, N.C. Gen. Stat. § 14-113.20(b)(1);

b. Drivers license, State identification card, or passport numbers, N.C. Gen. Stat. § 14-113.20(b)(2);

c. Financial account number, or credit card or debit card number, N.C. Gen. Stat. § 14-113.20(b)(3)-(6);

d. Personal Identification Code, electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names, digital signatures, N.C. Gen. Stat. § 14-113.20(b)(7)-(9);

e. "any other numbers or information that can be used to access a person's financial resources," N.C. Gen. Stat. § 14-113.20(b)(10); or

f. biometric data, fingerprints, passwords, legal surname prior to marriage, N.C. Gen. Stat. § 14-113.20(b)(11)-(14).

884. Defendants own, license and/or maintain computerized data that includes North Carolina Plaintiffs' and North Carolina Subclass Members' Personal Information.

885. Defendants' conduct, as alleged herein, violated the Identity Theft Protection Act of North Carolina, N.C. Gen. Stat. § 75-60.

886. Defendants were required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

887. Data Breach constituted a "Security breach" within the meaning of N.C. Gen. Stat. § 75-60.

888. The information compromised in the Data Breach constituted "personal identifying information" within the meaning of N.C. Gen. Stat. § 75-60.

889. Defendants violated N.C. Gen. Stat. § 75-60 by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class members, whose personal identifying information was, or reasonably believed to have been, acquired by an unauthorized person.

890. Specifically, Defendants collected and stored North Carolina Plaintiffs' and the North Carolina Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing North Carolina Plaintiffs' and the North Carolina Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

891. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of

multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

892. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect North Carolina Plaintiffs' and the North Carolina Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to North Carolina Plaintiffs' and the North Carolina Subclass's Personal Information. While Defendants profited off of North Carolina Plaintiffs' and the North Carolina Subclass's data, they failed to take the necessary measures to protect it, leaving North Carolina Plaintiffs and the North Carolina Subclass at significant and foreseeable risk of harm.

893. Although Defendants collectively acted in violation of the Identity Theft Protection Act of North Carolina, each Defendant also separately violated the Identity Theft Protection Act of North Carolina by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated the Identity Theft Protection Act of North Carolina by developing the legacy server subject to the breach, including collecting and aggregating North Carolina Plaintiffs' and the North Carolina Subclass's Personal

Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

894. Optum also independently violated the Identity Theft Protection Act of North Carolina. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview, and specifically, was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

895. Lastly, UHG also independently violated the Identity Theft Protection Act of North Carolina. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for

and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

896. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

897. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to

adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the Subclass at significant risk of harm.

898. Consequently, Defendants, collectively, and each, independently, took actions in violation of the Identity Theft Protection Act of North Carolina.

899. As a result of those unlawful and unfair business practices, North Carolina Plaintiffs and the North Carolina Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

900. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

901. North Carolina Plaintiffs and the North Carolina Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on North Carolina Plaintiffs and the North Carolina Subclass. Without the use of adequate data security, North Carolina Plaintiffs and the North Carolina Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

902. North Carolina Plaintiffs and the North Carolina Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXIII

Violation of Or. Rev. Stat. §§ 646.608, *et seq*.,

(On behalf of Oregon Plaintiffs and the Oregon Subclass against all Defendants)

903. Oregon Plaintiffs, individually and on behalf of the Oregon Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

904. Oregon Revised Statute § 646.608 prohibits any person engaging in an unlawful practice in the course of their business. A person does so by engaging in "unfair or deceptive conduct in trade or commerce."

905. Defendants violated Oregon Revised Statute § 646.608 by engaging in conduct that constituted "unfair or deceptive conduct."

906. Specifically, Defendants collected and stored Oregon Plaintiffs' and the Oregon Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Oregon Plaintiffs' and the Oregon Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

907. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

908. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Oregon Plaintiffs' and the Oregon Subclass's highly sensitive and

private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Oregon Plaintiffs' and the Oregon Subclass's Personal Information. While Defendants profited off of Oregon Plaintiffs' and the Oregon Subclass's data, they failed to take the necessary measures to protect it, leaving Oregon Plaintiffs and the Oregon Class at significant and foreseeable risk of harm.

909. Although Defendants collectively acted in violation of Oregon Revised Statute § 646.608, each Defendant also separately violated the statute by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged after UHG's acquisition of Change Healthcare, violated Oregon Revised Statute § 646.608 by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

910. Optum also independently violated Oregon Revised Statute § 646.608. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change

Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

911. Lastly, UHG also independently violated Oregon Revised Statute § 646.608. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare, and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

912. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors

"oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

913. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Oregon Plaintiffs and the Oregon Subclass at significant risk of harm by failing to reasonably secure it.

914. Consequently, Defendants collectively and each independently took actions in violation of the Act.

915. As a result of those unlawful and unfair business practices, Oregon Plaintiffs' and the Oregon Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information

was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

916. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

917. Oregon Plaintiffs and the Oregon Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Oregon Plaintiffs and the Oregon Subclass. Without the use of adequate data security, Oregon Plaintiffs and the Oregon Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

918. Oregon Plaintiffs and the Oregon Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the

law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXIV

Violation of Rhode Island Unfair Trade Practice and Consumer Protection Act, R.I. Gen. Laws § 6-13.1-1, *et seq*.

(On behalf of Rhode Island Plaintiffs and the Rhode Island Subclass against all Defendants)

919. Rhode Island Plaintiffs, individually and on behalf of the Rhode Island Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

920. The Rhode Island Unfair Trade Practices and Consumer Protection Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." R.I. Gen. Laws Ann. § 6-13.1-2. Under the statute, "unfair or deceptive acts or practices" include "[e]ngaging in any act or practice that is unfair or deceptive to the consumer." R.I. Gen. Laws Ann. § 6-13.1-1(6)(xiii). The statute expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. See R.I. Gen. Laws Ann. § 6-13.1-3.

921. Rhode Island Plaintiffs and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3). Rhode Island Plaintiffs and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws Ann. § 6-13.1-5.2(a) as each purchased goods and/or services primarily for personal, family, and/or household purposes and suffered and will continue to suffer an "ascertainable loss of

money or property, real or personal, as a result of the use or employment by another person of a method, act, or practice declared unlawful by" this statute.

922. Defendants advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws §§ 6-13.1-1(5) and 6-13.1-1(6)(xiii).

923. Defendants engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2 and 6-13.1-1(6)(xiii).

924. Specifically, Defendants collected and stored Rhode Island Plaintiffs' and the Rhode Island Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Rhode Island Plaintiffs' and the Rhode Island Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

925. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of

multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

926. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Rhode Island Plaintiffs' and the Rhode Island Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Rhode Island Plaintiffs' and the Rhode Island Subclass's Personal Information. While Defendants profited off of Rhode Island Plaintiffs' and the Rhode Island Subclass's data, they failed to take the necessary measures to protect it, leaving Rhode Island Plaintiffs and the Rhode Island Subclass at significant and foreseeable risk of harm.

927. Although Defendants collectively acted in violation of the Rhode Island Unfair Trade Practice and Consumer Protection Act, each Defendant also separately violated the Rhode Island Unfair Trade Practice and Consumer Protection Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged following UHG's acquisition of Change Healthcare, violated the Rhode Island Unfair Trade Practice and Consumer Protection Act by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the Rhode

Island Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

928. Optum also independently violated the Rhode Island Unfair Trade Practice and Consumer Protection Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum." During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

929. Lastly, UHG also independently violated the Rhode Island Unfair Trade Practice and Consumer Protection Act. UHG controlled and oversaw Change Healthcare

generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare, and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

930. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

931. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information

of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Rhode Island Plaintiffs and the Rhode Island Subclass at significant risk of harm.

932. Consequently, Defendants collectively and each independently took actions in violation of the Rhode Island Unfair Trade Practice and Consumer Protection Act.

933. As a result of those unlawful and unfair business practices, Rhode Island Plaintiffs' and the Rhode Island Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

934. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Rhode Island Plaintiffs and the Rhode Island Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data

Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

935. Rhode Island Plaintiffs and the Rhode Island subclass also remain at heightened risk of future injury because their Personal Information resides with Defendants and, further, because Defendants continue to gather new medical information on Rhode Island Plaintiffs and the Rhode Island Subclass. Without the use of adequate data security, Rhode Island Plaintiffs and the Rhode Island Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

936. Rhode Island Plaintiffs and the Rhode Island Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXV

Violation of South Carolina Unfair Trade Practices Act (SCUTPA), SC ST § 35-5-20

(On behalf of South Carolina Plaintiffs and the South Carolina Subclass against all Defendants)

937. The South Carolina Plaintiffs, individually and on behalf of the South Carolina Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

938. South Carolina's Unfair Trade Practices Act (SCUTPA) prohibits any person from engaging in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. SC ST § 39-5-20.

939. Defendants violated SCUTPA by engaging in conduct that constituted "unfair or deceptive acts or practices", by collecting and storing Plaintiffs' and the South Carolina Subclass's Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiffs' the South Carolina Subclass's information, and failing to adequately segment the sensitive data from other parts of Change's servers and networks.

940. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without two-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of two factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

941. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes an immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect South Carolina Plaintiffs' and the South Carolina Subclass's highly

sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to South Carolina Plaintiffs' and the South Carolina Subclass's Personal Information. While Defendants profited off of South Carolina Plaintiffs' and the South Carolina Subclass's data, they failed to take the necessary measures to protect it, leaving South Carolina Plaintiffs and the South Carolina Subclass at significant and foreseeable risk of harm.

942. Although Defendants collectively acted in violation of SCUTPA, each Defendant also separately violated the SCUTPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change, violated SCUTPA by developing the legacy server subject to the breach, including collecting and aggregating Plaintiffs' and the South Carolina Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

943. Optum also independently violated SCUTPA. Upon its acquisition of Change Healthcare, Optum oversaw Change and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's

purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

944. Lastly, UHG also independently violated SCUTPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

945. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors

"oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

946. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare, they put Plaintiffs and the South Carolina Subclass at significant risk of harm.

947. Consequently, Defendants collectively, and each independently, took actions in violation of SCUTPA.

948. As a result of those unlawful and unfair business practices, Plaintiffs and the South Carolina Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

949. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

950. South Carolina Plaintiffs and the South Carolina Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on South Carolina Plaintiffs and the South Carolina Subclass. Without the use of adequate data security, South Carolina Plaintiffs and the South Carolina Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

951. South Carolina Plaintiffs and the South Carolina Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper pursuant to SC ST § 39-5-140.

COUNT XXXVI

Violation of SC ST § 39-1-90

(On behalf of South Carolina Plaintiffs and the South Carolina Subclass against all Defendants)

952. South Carolina Plaintiffs, individually and on behalf of the South Carolina Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

953. A person conducting business in South Carolina, and owning or licensing computerized data or other data that includes personal identifying 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 this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. SC ST § 39-1-90

954. Defendants are person conducting business in South Carolina and own or license computerized data that includes personal identifying information

955. Upon information and belief, included among the data made subject of the breach was South Carolina Plaintiffs and South Carolina Subclass Members' Personal Information which was not rendered unusable through encryption, redaction or other methods. SC ST § 39-1-90.

956. By statute, Defendants were required to provide notice "in the most expedient time possible and without unreasonable delay." SC ST § 39-1-90.

957. Defendants became aware of the data breach on February 21, 2024. By mid-March, Defendants supposedly gained possession of the original data set extracted by cybercriminals in the breach. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants failed to fully provide the required written notice to many affected persons for at least eight months. Defendants notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024 that it had mailed notices to approximately 100 million persons at that point and continued issuing notices after that date. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

958. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices were inadequate and failed to inform Plaintiffs and the Class as to whether they were impacted by the Data Breach. Because Plaintiffs and the Class had no direct relationship with Change Healthcare and no knowledge of whether Change Healthcare processed their insurance claims, Plaintiffs and the Class could not determine whether they were impacted by the Data Breach based on the public announcements. The Data Breach notices, in fact, reinforce that Plaintiffs could not have known whether they were impacted by a Data Breach of Change Healthcare. In the notices, Change Healthcare acknowledges that it was unable to identify from which medical provider or providers it obtained each individuals' medical information and, given that Change Healthcare could not make that determination, Plaintiffs lacked information to do so too.

959. Consequently, Plaintiffs and the Class did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred, which occurred at the earliest of five months after the breach and at the latest, over eight months later. That notice is insufficient under South Carolina law.

960. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated SC ST § 39-1-90.

961. As a direct and proximate result of Defendants' violations of SC ST § 39-1-90, South Carolina Plaintiffs and South Carolina Subclass Members suffered damages including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

962. South Carolina Plaintiffs and South Carolina Subclass Members seek relief under SC ST § 39-1-90, including actual damages and injunctive relief.

COUNT XXXVII

Violation of Vermont Consumer Fraud Act, Vt. Stat. Ann tit. 9, § 2451, et seq.

(On behalf of Vermont Plaintiffs and the Vermont Subclass against all Defendants)

963. Vermont Plaintiffs, individually and on behalf of the Vermont Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

964. The Vermont Consumer Fraud Act prohibits "unfair or deceptive acts or practices in commerce." Vt. Stat. Ann tit. 9, § 2453(a). The statute expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. See Vt. Stat. Ann tit. 9, § 2453(b).

965. Vermont Plaintiffs and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

966. Defendants' conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

967. Defendants are each a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

968. Defendants advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

969. Defendants engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of insurance and health benefits services in violation of Vt. Stat. Ann. tit. 9, § 2453.

970. Specifically, Defendants collected and stored Vermont Plaintiffs' and the Vermont Subclass's Personal Information. Defendants stored the Personal Information in

a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Vermont Plaintiffs' and the Vermont Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

971. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

972. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Vermont Plaintiffs' and the Vermont Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and

sale of data related to Vermont Plaintiffs' and the Vermont Subclass's Personal Information. While Defendants profited off of Vermont Plaintiffs' and the Vermont Subclass's data, they failed to take the necessary measures to protect it, leaving Vermont Plaintiffs and the Vermont Subclass at significant and foreseeable risk of harm.

973. Although Defendants collectively acted in violation of the Vermont Consumer Fraud Act, each Defendant also separately violated the Vermont Consumer Fraud Act by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, which merged after UHG acquired Change Healthcare, violated the Vermont Consumer Fraud Act by developing the legacy server subject to the breach, including collecting and aggregating Vermont Plaintiffs' and the Vermont Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

974. Optum also independently violated the Vermont Consumer Fraud Act. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be

subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

975. Lastly, UHG also independently violated the Vermont Consumer Fraud Act. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to satisfy.

976. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance

Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

977. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Vermont Plaintiffs and the Vermont Subclass at significant risk of harm by failing to reasonably secure it.

978. Consequently, Defendants collectively and each independently took actions in violation of the Vermont Consumer Fraud Act.

979. As a result of those unlawful and unfair business practices, Vermont Plaintiffs and the Vermont Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information over one hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

980. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Vermont Plaintiffs and the Vermont Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

981. Vermont Plaintiffs and the Vermont Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Vermont Plaintiffs and the Vermont Subclass. Without the use of adequate data security, Vermont Plaintiffs and the Vermont Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

982. Vermont Plaintiffs and the Vermont Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the

law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXVIII

Violation of Wash. Rev. Code § 19.86.020, *et. seq.*, Washington Consumer Protection Act

(On behalf of Washington Plaintiffs and the Washington Subclass against all Defendants)

983. Washington Plaintiffs, individually and on behalf of the Washington Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

984. The Washington Consumer Protection Act ("WA CPA") prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Wash. Rev. Code. § 19.86.020.

985. Defendants violated the WA CPA by engaging in unfair methods of competition and unfair acts.

986. Specifically, Defendants collected and stored Washington Plaintiffs' and the Washington Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Washington Plaintiffs' and the Washington Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

987. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

988. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Washinton Plaintiffs' and the Washington Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Washington Plaintiffs' and the Washington Subclass's Personal Information. While Defendants profited off of Washington Plaintiffs' and the Washington Subclass's data, they failed to take the necessary measures to protect it, leaving Washington Plaintiffs and the Washington Subclass at significant and foreseeable risk of harm.

989. Although Defendants collectively acted in violation of the WA CPA, each Defendant also separately violated the WA CPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the WA CPA by developing the legacy server subject to the Breach, including collecting and aggregating Washington Plaintiffs' and the Washington Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

990. Optum also independently violated the WA CPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare

implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

991. Lastly, UHG also independently violated the WA CPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

992. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

993. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare

adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further, profited off of the use of the data, they put Washington Plaintiffs and the Washington Subclass at significant risk of harm by failing to reasonably secure it.

994. Consequently, Defendants collectively and each independently took actions in violation of the WA CPA.

995. As a result of those unlawful and unfair business practices, Washington Plaintiffs and the Washington Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

996. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Washington Plaintiffs and the Washington Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value

of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

997. Washington Plaintiffs and the Washington Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Washington Plaintiffs and the Washington Subclass. Without the use of adequate data security, Washington Plaintiffs and the Washington Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

998. Washington Plaintiffs and the Washington Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XXXIX

Violation of Wash. Rev. Code § 19.255.010(1), *et. seq.*, Washington State Data Breach Notification Act

(On behalf of Washington Plaintiffs and the Washington Subclass against all Defendants)

999. Washington Plaintiffs, individually and on behalf of the Washington Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

1000. The Washington State Data Breach Notification Act ("Washington Breach Notification Act" requires notice and disclosure of any breach of the security of any system on which a Washington resident's information was acquired by an unauthorized person due to that personal information not having been secured. Wash. Rev. Code § 19.255.010(1).

1001. The notice required by the Washington Breach Notification Act must be provided no more than 30 days after discovery of the breach. Wash. Rev. Code § 19.255.010(8).

1002. Where a single breach affects more than 500 Washington residents, the business must notify the attorney general within 30 days. Wash. Rev. Code § 19.255.010(7).

1003. On February 12, 2024, ALPHV and is affiliates infiltrated Defendants' computer network and on February 21, 2024, they deployed ransomware on those networks.

1004. While the Data Breach occurred in February 2024, Defendants failed to fully provide the required written notice to many affected persons even eight months after the Data Breach, having notified the U.S. Dept. of Human Services Office of Civil Rights on October 22, 2024, that it had mailed notices to approximately 100 million persons at that point. According to Defendants' own statements, notifications did not even begin to be mailed until at least July 29, 2024, more than five months after the Data Breach.

1005. While Defendants made public representations of a Data Breach involving Change Healthcare, those public notices failed to inform Plaintiffs and the Class as to whether they were impacted by the Data Breach. Because Plaintiffs and the Class had no direct relationship with Change Healthcare, and no knowledge of whether Change Healthcare processed their insurance claims, Washington Plaintiffs and the Washington Subclass could not determine whether they were impacted by the Data Breach based on the public announcements. Washington Plaintiffs and the Washington Subclass did not know they were impacted by the Data Breach until they received direct notice several months after the breach occurred.

1006. The failure by Defendants to timely notify Washington Plaintiffs and the Washington Subclass of their information being exposed and/or exfiltrated in the Data Breach has caused Washington Plaintiffs and the Washington Subclass injury, including: the inability to protect themselves in the intervening months between Defendants' discovery of the Data Breach and their finally receiving notice; and the increased proliferation of their information on the dark web or other venues between Defendants'

discovery of the Data Breach and the notification to Plaintiffs and the Washington Subclass.

1007. Washington Plaintiffs and the Washington Subclass are statutorily entitled to bring a private cause of action under the Washington Breach Notification Act as consumers. Wash. Rev. Code § 19.255.040(3)(a).

1008. Washington Plaintiffs and the Washington Subclass are also statutorily entitled to injunctive relief for violation of the Washington Breach Notification Act. Wash. Rev. Code § 19.255.040(3)(b).

COUNT XL

Violation of Wis. Stat. §§ 146.81, *et seq.*,

(On behalf of the Wisconsin Plaintiffs and the Wisconsin Subclass on behalf of all Defendants)

1009. Wisconsin Plaintiffs, individually and on behalf of the Wisconsin Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

1010. Wisconsin law requires that patient healthcare records remain confidential and permits the release of those records only to designated persons "with the informed consent of the patient or of a person authorized by the patient." Wis. Stat. § 146.82.

1011. Wisconsin Plaintiffs' and the Wisconsin Subclass's Personal Information are "health care records" as defined by Wis. Stat. § 146.81(4).

1012. Defendants violated Wis. Stat. §§ 146.81, *et seq*. when it compromised, allowed access to, and released, patient healthcare records and PHI to third parties without the informed consent or authorization of Wisconsin Plaintiffs and the Wisconsin Subclass. Defendants do not and does not have express or implied consent to allow access to, or

release of, Wisconsin Plaintiffs' and the Wisconsin Subclass's Personal Information, including their medical records.

1013. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Wisconsin Plaintiffs and the Wisconsin Subclass suffered significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

1014. Wisconsin Plaintiffs and the Wisconsin Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XLI

Violation of Wyo. Stat. Ann. § 40-12-101, Wyoming Consumer Protection Act

(On behalf of Wyoming Plaintiffs and the Wyoming Subclass against all Defendants)

1015. Wyoming Plaintiffs, individually and on behalf of the Wyoming Subclass, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

1016. Wyoming's Consumer Protection Act ("WY CPA") provides that a person engages in a deceptive trade practice if during the course of their business and in connection with a consumer transaction they engage "in unfair or deceptive acts or practices." Wyo. Stat. Ann. § 40-12-105(xv).

1017. Defendants violated the WY CPA by engaging in conduct that constituted unfair acts and practices.

1018. Specifically, Defendants collected and stored Wyoming Plaintiffs' and the Wyoming Subclass's Personal Information. Defendants stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Wyoming Plaintiffs' and the Wyoming Subclass's information, and failing to adequately segment the sensitive data from other parts of Change Healthcare's servers and networks.

1019. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, contrary to UHG's, Optum's, and

Change Healthcare's own policies, access to the breached legacy database was possible without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information. Defendants acknowledged that the lack of multi-factor authentication was a significant cybersecurity failure and is inconsistent with reasonable data security practices.

1020. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Change Healthcare stored concerning one-third of the United States population, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over one hundred million people. That is especially true because, despite failing to reasonably protect Wyoming Plaintiffs' and the Wyoming Subclass's highly sensitive and private Personal Information, Defendants gained significant profit from that information. Indeed, a significant part of Defendants' revenue was the "unfettered" use, analysis, and sale of data related to Wyoming Plaintiffs' and the Wyoming Subclass's Personal Information. While Defendants profited off of Wyoming Plaintiffs' and the Wyoming Subclass's data, they failed to take the necessary measures to protect it, leaving Wyoming Plaintiffs and the Wyoming Subclass at significant and foreseeable risk of harm.

1021. Although Defendants collectively acted in violation of the WY CPA, each Defendant also separately violated the WY CPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Change Healthcare and Optum Insight, both of which merged following UHG's acquisition of Change Healthcare, violated the WY CPA by developing the legacy server subject to the breach, including collecting and aggregating

Wyoming Plaintiffs' and the Wyoming Subclass's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Change Healthcare failed to follow its own policies, and those of Optum and UHG, which required it to put in place certain measures to protect patient data like multi-factor authentication. Furthermore, Change Healthcare's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to leverage compromised credentials and move laterally within the system.

1022. Optum also independently violated the WY CPA. Upon its acquisition of Change Healthcare, Optum oversaw Change Healthcare and its activities, including its aggregation, collection, and maintenance of patient data. Change Healthcare was placed under Optum's purview and was merged with Optum Insight. In fact, Change Healthcare rebranded after the acquisition to list itself as "Part of Optum". During Andrew Witty's congressional testimony, he acknowledged that Change Healthcare would be subject to Optum's incident response plan and its cybersecurity policies, demonstrating Optum's oversight and control over Change Healthcare. In SEC filings, Optum further represented that it would take measures to protect the Personal Information within Change Healthcare's possession upon its acquisition. Optum's failure to ensure Change Healthcare implemented its cybersecurity policies and put in place reasonable safeguards to protect the highly sensitive data Change Healthcare stored were unfair and unlawful acts.

1023. Lastly, UHG also independently violated the WY CPA. UHG controlled and oversaw Change Healthcare generally, and its cybersecurity specifically. Upon acquiring Change Healthcare, UHG was responsible for and oversaw the process of upgrading and

modernizing Change Healthcare's technology. UHG acknowledged, during congressional testimony, that it had an obligation under state and federal law to protect the patient information stored by Change Healthcare and Witty stated UHG took that obligation very seriously. UHG also acknowledged it had cybersecurity policies, including policies that required multi-factor authentication, that Change Healthcare was required to implement.

1024. UHG described the extent to which it oversaw Change Healthcare's cybersecurity, including, among other things: constantly assessing and improving capabilities; working with key technology partners; sharing information about security threats and best practices; running continuous penetration tests; and providing external support to Change Healthcare. Witty also noted UHG's experienced Board of Directors "oversee" "risk management" and "cybersecurity" and that its Audit and Finance Committee also "oversees cybersecurity risks." Demonstrating its control, UHG took responsibility for investigating and responding to the Data Breach.

1025. UHG, like Optum and Change Healthcare, took unfair and unlawful acts with respect to Change Healthcare's cybersecurity. Despite knowing of the substantial amount of data Change Healthcare controlled and stored (and indeed, that data being a principal reason for the acquisition of Change), UHG failed to prioritize ensuring Change Healthcare adequately secured that information. That is evidenced by the fact that, a year and a half after acquiring Change Healthcare, UHG had failed to take basic security steps, including placing multi-factor authentication on accounts with access to the healthcare information of one-third of the U.S. While Defendants saved money and resources by declining to adequately secure the information they acquired from Change Healthcare and, further,

profited off of the use of the data, they put Wyoming Plaintiffs and the Wyoming Subclass at significant risk of harm by failing to reasonably secure it.

1026. Consequently, Defendants collectively and each independently took actions in violation of the WY CPA.

1027. As a result of those unlawful and unfair business practices, Wyoming Plaintiffs and the Wyoming Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of over one-hundred million patients. Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

1028. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Wyoming Plaintiffs and the Wyoming Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach;

and (10) a continued substantial and imminent risk of the misuse of their Personal Information.

1029. Wyoming Plaintiffs and the Wyoming Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Wyoming Plaintiffs and the Wyoming Subclass. Without the use of adequate data security, Wyoming Plaintiffs and the Wyoming Subclass remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

1030. Wyoming Plaintiffs and the Wyoming Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

1031. The Court should also award reasonable attorneys' fees to Wyoming Plaintiffs and the Wyoming Subclass pursuant to Wyo. Stat. Ann. § 40-12-108(b).

PRAYER FOR RELIEF

1032. WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. For a declaration of rights regarding the reasonable protection of Plaintiffs' Personal Information that remains in Defendants' possession and maintenance;

c. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Personal Information;

d. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

e. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

f. Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiffs and the Class;

g. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 15, 2025

s/Daniel E. Gustafson

Daniel E. Gustafson (#202241)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com

Plaintiffs' Overall Lead Counsel

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
100 Washington Avenue S., Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7900
bbleichner@chestnutcambronne.com

Brian C. Gudmundson
ZIMMERMAN REED LLP
1100 IDS Center
Minneapolis, MN 55402
Telephone: (612) 341-0400
Brian.Gudmundson@zimmreed.com

Patient Track Co-Lead Counsel

Shawn M. Raiter
LARSON-KING LLP
30 East Seventh Street, Suite 2800
St. Paul, MN 55101
Telephone: (651) 312-6500
sraiter@larsonking.com

MDL Liaison Counsel

Melissa S. Weiner (Co-Chair)
PEARSON WARSHAW, LLP
328 Barry Avenue S., Suite 200
Wayzata, MN 55391
Telephone: (612) 389-0601
mweiner@pwfirm.com

Gary F. Lynch (Co-Chair)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com

Caroline Fabend Bartlett
CARELLA BYRNE CECCHI BRODY AGNELLO P.C.
5 Becker Farm Road
Roseland, NJ 07068
Telephone: (973) 422-5557
cbartlett@carellabyrne.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
CSchaffer@lfsblaw.com

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 250-3370
ssoneji@tzlegal.com

Erin Green Comite
SCOTT + SCOTT ATTORNEYS AT LAW
156 South Main Street
Colchester, CT 06415
Telephone: (860) 537-5537
ecomite@scott-scott.com

Ronald Podolny
MORGAN AND MORGAN, P.A.
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 225-6749
ronald.podolny@forthepeople.com

Gary Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
gklinger@milberg.com

Jason Rathod
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302
Washington, DC 20002
Telephone: (202) 470-3520
jrathod@classlawdc.com

Ronnie Spiegel
JOSEPH SAVERI LAW FIRM
601 California Street, Suite 1000
San Francisco, CA 94108
Telephone: (415) 500-6800
rspiegel@saverilawfirm.com

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: (504) 525-8100
amurray@murray-lawfirm.com

Kennedy M. Brian
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 286-1607
kpb@federmanlaw.com

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Amanda Christenson et al.
see attachment for full list

(b) County of Residence of First Listed Plaintiff Madison, AL

(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Daniel E. Gustafson
Gustafson Gluek PLLC
Canadian Pacific Plaza, 120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
612-333-8844

DEFENDANTS

UnitedHealth Group Incorporated, Optum, Inc., Optum Insight, LLC and Change Healthcare, Inc.

County of Residence of First Listed Defendant Hennepin, MN

(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

TORTS

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

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

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

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

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

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

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

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

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

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

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

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

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332

Brief description of cause:
Class action deriving from data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5000000

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Donovan W. Frank DOCKET NUMBER 0:24-md-3108

DATE
01/15/2025

SIGNATURE OF ATTORNEY OF RECORD
s/ Daniel E. Gustafson

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Plaintiffs:

1. Amanda Christenson
2. Taisha Dixon
3. Tracy Anne Phillips
4. Paul Avery
5. Jacqueline Jackson
6. Robin Dugan
7. Tawfik Mammad
8. Zoe Madonna
9. Kali Warren
10. Bethany Conley
11. Brittany Meadows
12. Olga Diatlova
13. Lashanden Darby
14. Edith Antonio
15. Amanda Rape
16. Deana Leffers
17. M.O.
18. Joshua Lowe
19. Rene Sims
20. Hailey Kleinheksel
21. Michelle Carter
22. Marissa Hatfield
23. Cedric Bonier
24. Jan Merrill
25. Richard Seibert
26. Michael Paul
27. DeBorah Evans
28. Lisa Brooks
29. David Powers
30. Roxanne Allen
31. Patricia Baggett
32. Kenya Jones
33. Edwin Hoag
34. Richard Schwalbe
35. Delmar Kentner
36. Dawn Duncan
37. Rosa Rubera
38. Matthew Loforese
39. Carol Slack
40. Rachael Schiller
41. Tristano Korlou

42. Patricia Donadio
43. James Morgan
44. Kaela Poitra
45. Autumn Abramczyk
46. Anna Griffith
47. Preslee Thorne
48. Robin Lanier
49. Ashley Harbon
50. Kim Kaehler
51. Sally Kirkpatrick
52. Tess Bussick
53. Lori Tynch
54. Polly Rush
55. Anna Lovell
56. Christina Estep
57. Alfred Williams, Sr.
58. Angela Johnson
59. Trudy Agres
60. Leigh Thompson (Tom) Hanes
61. J'Andre Ivory
62. Harry Knopp
63. Mark Wetzel
64. Luke Anderson
65. Lauren Fossen