

IN THE DISTRICT COURT OF
LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA, *ex rel.*
MICHAEL T. HILGERS, Attorney
General,

Plaintiff,

v.

CHANGE HEALTHCARE INC.,
UNITEDHEALTH GROUP
INCORPORATED, and OPTUM,
INC.,

Defendants.

COMPLAINT

The State of Nebraska, *ex rel.* Michael T. Hilgers, Nebraska Attorney General, by and through the undersigned attorneys (“Attorney General,” “State of Nebraska,” or “State”) brings this action against Defendants Change Healthcare Inc. (“Change”), UnitedHealth Group Incorporated (“UHG”), and Optum, Inc. (“Optum”) for violations of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601 *et seq.* (“CPA”), the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.*, and the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.* (“UDTPA”) stemming from a data breach that exposed the personal information and electronic protected health information of approximately 575,000 Nebraskans¹ and halted critical operations of

¹ Defendants claim to be currently unable to ascertain the total number of affected Nebraska consumers. The U.S. Department of Health and Human Services reports that, as of October 22, 2024, Defendants have sent approximately 100 million notices to affected individuals—approximately 29% of the United States. Extrapolating that number to Nebraska yields approximately 575,000 affected Nebraskans.

scores of Nebraska healthcare providers. In support thereof, the State of Nebraska alleges the following:

BACKGROUND

1. Defendant Change is one of the largest processors of prescription medications and insurance claims in the nation. It processes approximately half of all medical claims in the United States for around 900,000 physicians, 67,000 pharmacies, 5,500 hospitals, and 600 laboratories. In Nebraska alone, Change processes millions of claims per year.² It is owned by Defendant UHG, which acquired it in 2022 and at all relevant times had control over its IT operations and systems. And it is operated by Defendant Optum.

2. On February 21, 2024, UHG filed a Form 8-K with the United States Securities and Exchange Commission, in which it quietly announced that it had identified a “suspected nation-state associated cyber security threat actor had gained access to some of [Change’s] information technology systems.”

3. In that same filing, UHG claimed it had: (1) “isolated” the impacted systems; (2) retained experts; and (3) “notified customers, clients, and certain government agencies.” This, however, dramatically understated the problem.

4. In reality, what UHG tried to describe as a relatively benign “isolat[ion]” of Change’s systems was a total shutdown of the Change platform. The data breach and subsequent shutdown of services, without warning and without adequate backup and redundancies, was so great that it sent the entire U.S. healthcare system into a virtual meltdown.

5. Because Change’s systems were outdated and lacked appropriate segmentation and redundancies, in violation of company

² From July 2021 to June 2022, Change processed at least 441 million claims in total. See *The Change Healthcare 2022 Revenue Cycle Denials Index*, Change Healthcare, 6, <https://www.changehealthcare.com/insights/denials-index>.

policies, federal privacy requirements, and basic standards of enterprise information security, UHG disabled Change's processing services entirely, blocking countless transactions from the end of February through the middle of March, crippling Nebraskan healthcare providers and halting care for approximately 575,000 Nebraskans. Prior authorizations for pharmaceuticals and medical care were halted, resulting in prescriptions going unfilled and patient care being delayed. And Scammers began contacting patients, posing as representatives of hospitals throughout Nebraska and asking for patients' credit card numbers to issue supposed refunds.

6. Providers bore the brunt of providing care without compensation for the duration of the system outage, and thereafter as backlogs were slowly cleared. One cybersecurity firm estimated that some larger health systems lost more than \$100 million *a day* during the outage. In a survey by the American Hospital Association of about 1,000 hospitals, 74% percent of those hospitals reported direct impacts to patient care.

7. Over the course of many months, and following a Congressional inquiry, the truth of the attack—its preventability, the actions by Defendants that exacerbated it at the expense of Nebraska's citizens and those who provide them with critical healthcare services and life-saving medications, and the harm suffered by Nebraskans—began to come to light.

8. Despite all of this, and in contravention of Nebraska law, Defendants did not even begin to notify consumers via direct communications that their data had been stolen from Change's systems until the end of July 2024—almost five months after Defendants discovered the breach—and only after the Nebraska Attorney General had requested information on Change's efforts to provide notice. Defendants still have not directly notified all affected Nebraskans.

9. The Attorney General brings this action to vindicate the rights of Nebraska citizens and protect their most sensitive personal, medical, and financial information in accordance with Nebraska's laws.

PUBLIC INTEREST

10. The Attorney General believes this action to be in the public interest of the citizens of the State of Nebraska and brings this lawsuit pursuant to the CPA, the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, the UDTPA, and his statutory and common law authority, powers, and duties.

PARTIES

11. The State of Nebraska, by and through its Attorney General, brings this action as the Chief Law Enforcement Officer of the State of Nebraska charged, *inter alia*, with the enforcement of the CPA, the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, and the UDTPA. The Attorney General brings this action on behalf of the people of the State of Nebraska to protect the state, its general economy, and its residents from Defendants' unlawful business practices.

12. Defendant Change Healthcare Inc. is incorporated in Delaware with its principal place of business in Nashville, Tennessee. It became a subsidiary of UHG in 2022 and is operated by Optum, another UHG subsidiary. It provides services for at least two dozen hospitals and healthcare systems throughout Nebraska, and, in the course of conducting its business, it receives, processes, transmits, and stores sensitive personal, medical, and financial information and electronic protected health information of Nebraska residents.

13. Defendant Optum, Inc. maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware. It regularly transacts business in Nebraska through its operation of Change, and it also regularly transmits personal, medical, and financial information and electronic protected health information through its operation of Change.

14. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota. UHG exercises control over Change's cybersecurity and IT systems, including the systems impacted by the

events described herein that housed the personal, medical, and financial information and electronic protected health information of Nebraska residents and entities.

JURISDICTION AND VENUE

15. At all times relevant to this Complaint, Defendants were in trade and commerce affecting consumers in Nebraska insofar as they provided health care clearinghouse and related services to health care providers and consumers in Nebraska. Defendants were also in possession and/or had control over sensitive personal information of Nebraska residents.

16. This Court has personal jurisdiction over Defendants because the conduct and injuries from which the Complaint arose took place in Nebraska, harmed Nebraskans, and specifically targeted Nebraskans.

17. This Court has jurisdiction over the subject matter of this action under Neb. Rev. Stat. §§ 59-1608.01, 87-303.05(1), and 87-806 because Defendants, directly and through their subsidiaries, transacted business within the State of Nebraska at all times relevant to this Complaint.

18. The Attorney General, as Nebraska's Chief Law Enforcement Officer, is expressly authorized to enforce Nebraska's consumer protection laws, including the CPA, the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, and the UDTPA. Neb. Rev. Stat. §§ 59-1608; 59-1614; 87-806; 87-303.05; 87-303.11.

19. In addition to his express statutory authority, the Attorney General has standing to bring a legal action, in the name of the State, when the object of that action is a suit to vindicate the public interest.

20. Venue for this action properly lies in Lancaster County, Nebraska, pursuant to Neb. Rev. Stat. §§ 59-1608.01 and 87-806.

FACTS

A. Defendants Process and Store Sensitive Personal Information

21. Change acts as a digital clearinghouse for the healthcare industry, providing revenue and payment cycle management services that connect patients, providers, pharmacies, and payers within the healthcare pipeline. This includes processing insurance claims and billing for more than 15 billion medical claims each year.

22. In the course of its business, Change receives, processes, and stores electronic protected health information of tens of millions of Americans, including hundreds of thousands of Nebraskans.

23. The information Change receives, processes, and stores is subject to the requirements of not only Nebraska law, but also the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 (“HIPAA”). These laws require the implementation of “security procedures and practices . . . appropriate to the nature and sensitivity” of the personal information held or stored by an entity, taking into account “the nature and size of, and resources available to, the business.” Neb. Rev. Stat. § 87-808; *see also* HIPAA, 45 CFR Part 160 and Subparts A and C of Part 164.

24. As one of the largest processors of sensitive health information in the nation, Change, its parent entity UHG (which sees revenues in excess of \$370 billion annually—more than 24 times the budget of the State), and its operating entity Optum recognized and acknowledged the importance of proper data handling and up-to-date security systems.

25. Defendants had numerous Enterprise Information Security policies in place at the time of the breach that should have prevented the very harms at issue here.

26. They had a policy requiring Multi-Factor Authentication (“MFA”) on all user authenticated systems and before an employee (or non-employee) accessed protected or confidential information.

27. Defendants had a policy requiring [REDACTED]

[REDACTED]
That policy further required that [REDACTED]

28. Defendants’ policies required that [REDACTED]

[REDACTED]
Their policies further required [REDACTED]

29. And Defendants had requirements in place to [REDACTED]

30. Defendants’ public representations also illustrated that they recognized and acknowledged the importance of proper data handling and up-to-date security systems.

31. For example, Change includes in its Code of Conduct, publicly available on its website, the following representations:

- (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.”

(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.”

32. And Change’s Global Privacy Notice, publicly available on its website, advertises:

(a) “Change Healthcare functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers at its primary business function, so Change Healthcare’s collection, use and disclosure of protected health information is guided by HIPAA and the terms of a business associate agreement and other contracts.”

(b) “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.”

33. That Global Privacy Notice also provides that “Change Healthcare is now a part of Optum,” and the contact information for “questions or complaints” related to the Global Privacy Notice is an Optum email and an Optum mailing address.

34. Change’s website likewise advertised (and still advertises) that it stores electronic protected health information in a manner that “meets or exceeds HIPAA Privacy and Security Rule requirements.”

35. Indeed, Change has an entire arm of its website dedicated to what it calls “HIPAA Simplified,” characterized as Change’s “one-stop portal for insight and guidance into healthcare administrative

simplification regulations, timelines, program updates, and other initiatives at the forefront of the healthcare industry.” That page links to a document titled Change’s “Commitment to Compliance,” which “provides assurance to our customers that applicable Change Healthcare products and services meet or exceed regulatory requirements.”

36. Another arm of Change’s website boasts Change’s “Accreditations & Certifications,” which purport to “demonstrate our continued commitment to assure that applicable Change Healthcare products and services meet industry and regulatory requirements and expectations.”

B. Hackers Access Change’s Systems and Exfiltrate Sensitive Data

37. On or about February 11, 2024, the user name and password for a low-level, customer support employee’s access to Change’s Citrix portal (the “Portal”) were posted in an Telegram group chat that advertises the sale of stolen credentials.

38. The Portal was a virtual desktop, where the employee could access the Change applications (as permitted by Change) needed to perform their job responsibilities. The account was a basic, user-level account: it only had access to specific applications and did not have administrator access or credentials.

39. On February 12, 2024, a hacker accessed the Portal via the username and password shared on the Telegram group chat, thus gaining entry to the basic, user-level account. From that limited account, the hacker was able to break into the server that hosted Change’s medication management application, SelectRX.

40. This access to systems critical to Change’s operations by a user-level account went undetected by Defendants until the hacker revealed itself when it began to encrypt Change’s systems over a week later, locking Change out of those systems.

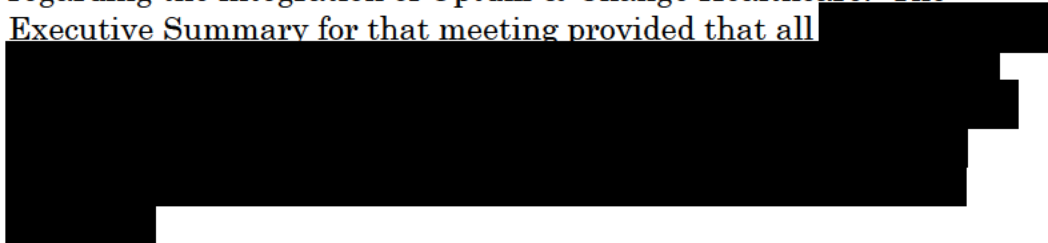
41. From there, the hacker created privileged accounts with administrator capabilities that permitted access to and deletion of any

and all files, changes to system configurations, and similar administrator-level activities. These actions went to the heart of the integrity of Change's most critical IT infrastructure, but still went undetected by Defendants.

42. Over the next nine days, the hacker navigated through Change'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 did detect the suspicious activity and try to block access.

43. The hacker continued to access the systems undetected and unimpeded. The hacker copied and exfiltrated terabytes of personal identifying information, financial account information, and protected health information for tens of millions of individuals and approximately 575,000 Nebraskans, including Social Security numbers, driver's licenses, state ID numbers, passport numbers, health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers), health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment), and/or billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due). These acts, too, went undetected until the hacker revealed itself.

44. Ironically, on February 13, 2024, the day after the attack began, Defendants' Executive Steering Committee held a meeting regarding the integration of Optum & Change Healthcare. The Executive Summary for that meeting provided that all



C. Change and UHG Finally Learn of the Attack

45. It was not until February 21, 2024, when the hacker deployed ransomware on Change's systems causing outages and disruptions, that Defendants became aware of a cybersecurity threat to Change's systems.

46. That day, in response, Defendants took Change's systems offline. That is, the hacker's infiltration of Change's systems was so severe that Change's only response was to shut down its primary *and* secondary systems.

47. On or about February 26, 2024, the ransomware group BlackCat/ALPHV ("BlackCat") claimed responsibility for the attack. Change later confirmed that BlackCat had represented itself as responsible for the attack, and had claimed to have stolen terabytes of data.

48. On or about March 3, 2024, UHG made a bitcoin ransom payment to BlackCat of approximately \$22 million.

49. The payment of the ransom did not bring Change's systems back online or mitigate the harm done. Because Change was unable to check every system and interface for backdoors, and because Change's backup systems were also compromised, Change was unable to repair its systems. Instead, it opted to rebuild its systems from the ground up. Moreover, Change's redundancy systems were inadequate. This all caused additional delay in processing and harm to providers, payers, and consumers.

50. Notwithstanding the ransom payment, the data of approximately 575,000 Nebraskans remains in the hands of the hackers. In April 2024, another group began leaking files of stolen Change data after an affiliate of BlackCat alleged it never received their cut of Change's \$22 million payment.

D. Change's Security Flaws

51. All of the harm these attacks caused were avoidable had UHG and Change implemented straightforward security measures. As

of February of 2024, Change and UHG did not have systems, policies, and practices in place appropriate to secure and protect the volume and highly sensitive nature of the data being handled.

52. UHG acquired Change in 2022. UHG and Change were aware at the time of the acquisition that Change maintained outdated and highly-vulnerable systems, which they were purportedly in the process of updating at the time of the breach. For example, as UHG's CEO testified to Congress, aspects of Change's legacy systems used to process claims and payments were *up to 40 years old*. UHG's CEO also revealed that Change stored most of its data on physical servers, rather than cloud-based servers, which physical servers were less secure and lacked appropriate segmentation to take into account the sensitivity of the data at issue.

53. Among the outdated features of Change's systems was the lack of multi-factor authentication ("MFA"), a commonplace, basic security feature that requires a user to provide multiple, independent pieces of evidence to authenticate their identify and gain access to a system. In violation of UHG's own stated policies, the Change system that was targeted did not have MFA in place, meaning it could be accessed with nothing more than a username and password.

54. Once Change's system was infiltrated, the hacker 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. Moreover, Change's redundancies were also affected, inadequate, or both. This prevented the backup and redundancy systems from being effectively utilized to mitigate the damage from the breach.

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

E. Failure to Provide Notice

56. Defendants are and for months have been aware of what data was compromised, and they know consumers' information remains accessible on the dark web. They have, by their own account, over 100 data scientists analyzing the breach, purportedly working 24 hours-a-day, seven days-a-week. Yet, simple notices to consumers of the breach have still not been provided.

57. As late as July 2024, Defendants had still not provided notice to consumers that their data might have been compromised. In fact, Change did not begin to issue notices until it was required to respond to the Attorney General's CID. In light of this failure, the Attorney General published its own notice alerting Nebraskans to the breach.

58. As of the date of this complaint, the State of Nebraska believes that Defendants have still failed to provide written notice to many affected Nebraskans of the breach,³ leaving citizens more vulnerable to exploitation of the sensitive personal financial, health, and identifying information.

59. Defendants are in possession of affected Nebraska consumers' and commercial entities' emails, but have not notified via email *any* affected consumers nor many affected entities (and for those that have been notified, the delay in notification was unreasonable).

60. Nor have Defendants made a "[c]onspicuous posting of the notice on the[ir] website." The notice on Defendants' respective homepages are either non-conspicuous (UHG) or non-existent (Optum), and the notices were posted far too late—certainly not "without unreasonable delay."

³ As noted above, Defendants have declined to provide the State of Nebraska with information regarding the total number of affected Nebraskans, or notice provided to the same.

F. The Data Breach Upends the Healthcare System and Places Citizens at Risk

61. Defendants' conduct caused direct and significant economic harm to Nebraskans and Nebraska healthcare providers. The collapse of Change's systems halted a significant number of insurance-related private healthcare transactions in the State. The harms flowing from this unprecedented failure reverberated throughout the Nebraska healthcare system.

62. Scores of healthcare providers, e.g., hospitals, pharmacies, and care centers, could neither make insurance claims on behalf of their patients nor receive payments for claims. Claims that had already been submitted were paralyzed—providers could not access them, nor even pull them out of Change to resubmit them through a new processor.

63. Healthcare providers were faced with the choice of sticking with Change (and facing the uncertainties of trying to hold out until its system were restored) or switching to a different clearinghouse provider and incurring significant costs—both direct costs from the transition and staff time—to do so.

64. Most hospitals polled by the State reported a moderate to significant impact on their finances and/or operations. Affected providers spent valuable time and resources addressing the issues caused by Defendants' wrongful conduct, while at the same time struggling to provide patient care without payment.

65. Those that stuck with Change faced substantial cash flow shortages as they could not receive payments from claims (or even submit new claims). One hospital "had [a] near complete halt of any dollars coming in," and another had a "nearly complete stop on cash flow." Many relied on cash advances to stay afloat. Others turned to their reserve funds. At least one hospital cashed out investments and certificates of deposits to maintain operations—losing out on interest and investment income.

66. Those that switched clearinghouses, too, faced cash flow problems, in addition to the time and resources spent in converting to

a new provider. Some hospitals were forced to hire consultants or other third parties to facilitate their transition to new claims processors.

67. Even those facilities that switched claims processors relatively early on faced substantial claim denials from payors. These denials were based on the claims not being “timely”—i.e., that they were submitted or processed beyond the contracted time period during which providers would agree to pay for services provided. In some cases, providers wrote off hundreds of thousands of dollars as a result of claims being denied as untimely, through no fault of the provider, simply because claims were either tied up in Change’s systems, or not processed at all due to the outage.

68. At least one hospital had its price transparency services, which were through Change, deactivated. Another had issues getting prescriptions filled and still, at least as of June 2024, could not process claims for home medical equipment.

69. Among the hardest hit were Nebraska’s 62 critical access and rural hospitals—smaller facilities that provide critical care to rural and remote areas. These facilities provide essential medical care to underserved communities, but operate on extremely thin operating margins. They lack the negotiating power of larger systems and often operate under more restrictive payment terms, making them the most likely to suffer severe financial losses as a result of Change’s outage.

70. As Nebraska’s providers struggled to find ways to work around the outage—whether taking losses, finding new providers, or providing services without the prospect of timely payment—Change stayed largely silent. Providers reported minimal communication from Change or UHG—rather it was the Nebraska Hospital Association that became the primary source of information for providers about the outage.

71. These harms to providers flowed directly to Nebraskan patients, whose most sensitive personal information—which itself has value—has been stolen. Nebraskans were left without access to critical medications that they could not afford because pharmacies

could not verify patients' insurance. The ensuing chaos created substantial disruptions throughout the system.

72. Although Change's systems have largely been restored, Nebraskans are still incurring and are likely to incur direct economic damages from Defendants' conduct. Those whose stolen information is fraudulently used will incur related damages, such as:

(a) **Identity Theft:** Thieves combine real and fake information to create new identities, making it harder for victims to detect and resolve the issue. Thieves can also use victim's information to create new financial accounts, taking out loans and opening credit cards, which damage victim's credit scores. Worse yet, victims may be held responsible for repaying the debts incurred by thieves, which are exacerbated by late payment fees and penalties.

Reclaiming one's identity costs time and money, such as hiring a lawyer, subscribing to credit monitoring services, lost wages due to time spent resolving issues, or hiring a tax-professional for tax-related issues.

(b) **Medical Identity Theft:** Thieves use stolen identities to receive medical treatment, leading to incorrect medical records and potential loss of medical benefits for the victim. Victims can be denied coverage due to incorrect pre-existing conditions, and they can be billed for these medical services, which they never requested or received. Unpaid bills can be forwarded to debt collection companies.

Even when compromised medical identities are discovered, substantial time and resources must be expended to correct records and recover coverage and expenses. In the meantime, insurance premiums may rise and victim's legitimate medical claims could be denied by their insurance.

(c) **Financial Fraud:** Victims can lose money from unauthorized purchases and withdrawals from their accounts. These unauthorized acts can also lead to overdraft and related fees.

(d) **Damaged Credit:** All of the above issues can result in damage to victim's credit scores, resulting in higher interest rates on loans and credit cards, and costs for credit repair services to help restore credit scores. Poor credit can also lead to lost job opportunities.

73. Even those who are fortunate enough to avoid fraud may still incur harm, such as purchasing credit monitoring and identity theft protection, and the time and effort incurred in monitoring credit reports and financial account statements for indications of actual or attempted fraud or in implementing safety measures such as freezing and unfreezing credit score accounts.

74. The full scope and magnitude of the harm suffered by Nebraskans is still coming to light, but has already manifested as both widespread and significant:

CAUSES OF ACTION

Count 1: Violations of the CPA: Unfair Trade Practices

(Neb. Rev. St. § 59-1601, *et seq.*)

75. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

76. The CPA outlaws “[u]nfair methods of competition and unfair . . . acts or practices in the conduct of any trade or commerce.” Neb. Rev. St. § 59-1602.

77. Defendants, in the conduct of trade or commerce, engaged in unfair acts or practices in violation of Neb. Rev. St. § 59-1602, causing or resulting in their failure to secure or protect Nebraskan's personal, financial, and health information as follows:

- a. Defendants permitted disclosure of electronic protected health information in a manner inconsistent with requirements of Nebraska law, as well as HIPAA and its rules in at least the following ways:
 - i. Defendants failed to ensure the confidentiality of all electronic protected health information they

created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1) and Neb. Rev. St. § 87-808.

- ii. Defendants failed to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2) and Neb. Rev. St. § 87-808.
- iii. Defendants failed to 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) and Neb. Rev. St. § 87-808.
- iv. Defendants failed to ensure compliance by their workforces with the electronic protected health information security standard rules, in violation of 45 C.F.R. § 164.306(a)(4) and Neb. Rev. St. § 87-808.
- v. Defendants failed to 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) and Neb. Rev. St. § 87-808.
- vi. Defendants failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by Defendants, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A) and Neb. Rev. St. § 87-808.
- vii. Defendants failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, in violation of 45

C.F.R. § 164.308(a)(1)(ii)(B) and Neb.Rev.St. § 87-808.

- viii. Defendants failed to 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) and Neb. Rev. St. § 87-808.
- ix. Defendants failed to implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate, in violation of 45 C.F.R. § 164.308(a)(4)(ii)(B) and Neb. Rev. St. § 87-808.
- x. Defendants failed to implement policies and procedures to address security incidents, including addressing and responding to security incidents and mitigating their harmful effects, in violation of 164.308(a)(6)(i), (ii) and Neb. Rev. St. § 87-808.
- xi. Defendants failed to implement technical policies and procedures for electronic information systems that maintain electronic 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) and Neb. Rev. St. § 87-808.
- xii. Defendants failed to implement mechanisms to encrypt electronic protected health information whenever deemed appropriate, in violation of 45 C.F.R. § 164.312(e)(2)(ii) and Neb. Rev. St. § 87-808.
- xiii. Defendants failed to implement policies and procedures to maintain and document the security measures implemented to comply with security

regulations, in violation of 45 C.F.R. § 164.316(a) and Neb. Rev. St. § 87-808.

- b. Defendants failed to implement and maintain reasonable security practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, Defendants and their operations, in at least the following ways:
 - i. Failure to implement MFA.
 - ii. Failure to use sufficient “endpoint detection and response” (“EDR”) or “user behavioral analysis” (“UBA”) tools, allowing the threat actor to go undetected for 9 days.
 - iii. Failure to properly segment Change systems, both horizontally and vertically, allowing the threat actor to move easily across Change systems.
 - iv. Failure to have proper backup and redundancy systems in place causing the complete shutdown of Change’s system and substantial delay due to the need to rebuild systems from scratch.

78. Defendants’ unfair acts or practices were directed to each Nebraska resident for whom Change possessed data and to each entity that transacted with Change using Nebraskan’s personal, financial, or health information. Accordingly, each transaction that Change processed involving the personal, financial, or health information of a Nebraska resident or involving a Nebraska entity, each Nebraska resident’s personal, financial, or health information that Change possessed and was affected by the breach, and each transaction that a Nebraska entity would have processed but could not process because of the shutdown of Change’s system constitutes a separate violation of the statute.

79. These violations of Neb. Rev. St. § 59-1602 have impacted the public interest.

Count 2: Violations of the CPA: Deceptive Acts or Practices
(Neb. Rev. St. § 59-1601, *et seq.*)

80. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

81. The CPA outlaws “. . . deceptive acts or practices in the conduct of any trade or commerce.” Neb. Rev. St. § 59-1602.

82. Defendants, in the conduct of trade or commerce, engaged in deceptive acts or practices in violation of Neb. Rev. St. § 59-1602, causing or resulting in their failure to secure or protect Nebraskan’s personal, financial, and health information as follows:

- a. Contrary to their own well-publicized policies, procedures, and public representations regarding the security of Change’s systems and safety of consumers’ information, many—but not all—of which are identified in this Complaint, Defendants:
 - i. Failed to “follow[] [Change’s] privacy, security, and data and information protection policies” in storing and protecting electronic protected health information and personal identifying information;
 - ii. Failed to store and protect electronic protected health information and personal identifying information in a manner that “meets or exceeds HIPAA Privacy and Security Rule requirements” or other “regulatory requirements,” or that “meet[s] industry and regulatory requirements and expectations”;
 - iii. Failed to “regularly monitor [Change’s] systems to be sure that information is accessed and used for appropriate, authorized activities, to discover any new threats,” or to “monitor and control all electronic and computing devices used . . . to interact with [Change’s] internal networks and systems”;

- b. Defendants failed to timely notify consumers and affected entities of the breach.

83. Defendants' deceptive acts or practices were directed to each Nebraska resident for whom Change possessed data and to each entity which transacted with Change using Nebraskan's personal, financial, or health information. Accordingly, each transaction that Change processed involving the personal, financial, or health information of a Nebraska resident or involving a Nebraska entity, each Nebraska resident's personal, financial, or health information that Change possessed and was affected by the breach, and each transaction that a Nebraska entity would have processed but could not process because of the shutdown of Change's system constitutes a separate violation of the statute.

84. These violations of Neb. Rev. St. § 59-1602 impacted the public interest.

**Count 3: Violation of the Financial Data Protection and
Consumer Notification of Data Security Breach Act of 2006**
(Neb. Rev. St. § 87-801, *et seq.*)

85. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

86. Section 87-803 requires a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska to conduct in good faith, when it becomes aware of a breach of the security of the system, a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose.

87. The Act further requires, if the investigation determines that the use of information about Nebraska residents for an unauthorized purpose has occurred or is reasonably likely to occur, the commercial entity to give notice to affected Nebraska residents "as soon as possible and without unreasonable delay."

88. Defendants have known about the attack and the extent of the compromised data for months, but have failed to provide such notice with the requisite celerity.

89. Defendants waited until July 2024, at the earliest, to *begin* to send Nebraska consumers direct written notice.

90. Defendants failed to meaningfully communicate with providers regarding the full scope of the breach, impeding providers' ability to respond to patient concerns and to respond to the breach.

91. Nor has the "substitute notice" provision of Section 87-802(d), which requires email notice, been satisfied

92. Defendants' delay has been unreasonable in violation of the statute, and each such failure is its own violation of the statute.

**Count 4: Violation of the Financial Data Protection and
Consumer Notification of Data Security Breach Act of 2006**
(Neb. Rev. St. § 87-801, *et seq.*; Neb. Rev. Stat. §59-1602)

93. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

94. Section 87-808 of the Act required Defendants to implement and maintain reasonable security practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to them. A violation of this Section is considered a violation of Neb. Rev. Stat. §59-1602.

95. Defendants failed to implement and maintain reasonable security practices, as set forth *supra*.

96. Defendants are liable for a civil penalty for each violation pursuant to Neb. Rev. Stat. §59-1614.

Count 5: Violation of the UDTPA

(Neb. Rev. St. § 87-301, *et seq.*)

97. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

98. The UDTPA forbids deceptive trade practices as defined under the Act, including:

(a) Us[ing] deceptive representations . . . in connection with goods or services;

(b) Represent[ing] that goods or services have . . . characteristics . . . that they do not have;

(c) Represent[ing] that goods or services are of a particular standard, quality, or grade . . . if they are of another; and

(d) Knowingly mak[ing] a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.

Neb. Rev. Stat. § 87-302(a)(4), (5), (8), (15).

99. Defendants' advertisements and representations, many—but not all—of which are identified in this Complaint, regarding Change's protection of personal identifying information and electronic protected health information and its related compliance with regulations and industry standards were inaccurate and deceptive in violation of Neb. Rev. Stat. § 87-302(a)(4), (5), (8), (15).

100. By way of example, Defendants breached those provisions in the following ways:

(a) Defendants represented that Change would maintain sensitive personal information in accordance with HIPAA privacy rules and regulations, but did not, in violation of Neb. Rev. St. § 87-302(a)(4) and (15).

(b) Defendants represented that Change would store and protect electronic protected health information and personal identifying information “by following [Change’s] privacy, security, and data and information protection policies,” but did not, in violation of Neb. Rev. St. § 87-302(a)(4) and (15).

(c) Defendants represented that Change would store and protect electronic protected health information and personal identifying information in a manner that “meets or exceeds HIPAA Privacy and Security Rule requirements” or other “regulatory requirements,” or that “meet[s] industry and regulatory requirements and expectations,” but did not, in violation of Neb. Rev. St. § 87-302(a)(4) and (15).

(d) Defendants represented that Change would “regularly monitor [Change’s] systems to be sure that information is accessed and used for appropriate, authorized activities, to discover any new threats” and would “monitor and control all electronic and computing devices used ... to interact with our internal networks and systems,” but did not, in violation of Neb. Rev. St. § 87-302(a)(4) and (15).

(e) Defendants represented that they “implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse” when they did not, in fact, have such measures in place, in violation of Neb. Rev. St. § 87-302(a)(4) and (15).

(f) Defendants represented that their services had privacy and security characteristics and benefits that the services did not have, in violation of Neb. Rev. St. § 87-302(a)(5).

(g) Defendants represented that their services were of a particular standard and quality with respect to privacy

and security features when they were not, in violation of Neb. Rev. St. § 87-302(a)(8).

(h) Defendants otherwise made false or misleading statements in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public, in violation of Neb. Rev. St. § 87-302(a)(15).

101. Each of Defendants' deceptive trade practices were directed to each Nebraska resident for whom Change possessed data and to each entity which transacted with Change using Nebraskan's personal, financial, or health information. Accordingly, each transaction that Change processed involving the personal, financial, or health information of a Nebraska resident or involving a Nebraska entity, each Nebraska resident's personal, financial, or health information that Change possessed and was affected by the breach, and each transaction that a Nebraska entity would have processed but did not process because of the shutdown of Change's system constitutes a separate violation of the statute.

102. These violations of Neb. Rev. St. § 87-301 impacted the public interest.

**Count 6: Violation of the UDTPA
(Neb. Rev. Stat. § 87-303.01)**

103. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

104. An unconscionable act or practice by a supplier in connection with a consumer transaction is a violation of the UDPTA. Neb. Rev. Stat. § 87-303.01(1).

105. The unconscionability of an act or practice is a question of law for the court. Neb. Rev. Stat. § 87-303.01(2).

106. Change engaged in unconscionable acts or practices in violation of the UDTPA, Neb. Rev. Stat. § 87-303.01, by, without limitation:

(a) Failing to implement appropriate security policies, procedures, and practices in connection with the handling of sensitive personal information, including, but not limited to, failing to implement MFA, failing to properly segregate systems, and failing to update aging computer systems to ensure the security and integrity of consumer data.

(b) Misrepresenting the characteristics and qualities of Change's security policies, procedures, and practices in connection with the handling of sensitive personal information and Change's compliance with related rules, regulations, statutes, and standards.

(c) Failing to timely notify consumers and affected entities of the breach.

107. Each of Defendants' unconscionable acts or practices were directed to each Nebraska resident for whom Change possessed data and to each entity which transacted with Change using Nebraskan's personal, financial, or health information. Accordingly, each transaction that Change processed involving the personal, financial, or health information of a Nebraska resident or involving a Nebraska entity, each Nebraska resident's personal, financial, or health information that Change possessed and was affected by the breach, and each transaction that a Nebraska entity would have processed but did not process because of the shutdown of Change's system constitutes a separate violation of the statute.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter judgment against Defendants and enter an Order:

108. Finding that Defendants violated the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. §§ 87-803 and 87-808; the CPA, Neb. Rev. Stat. § 59-1602; and the UDTPA § 87-302-303 by engaging in the unlawful acts and practices alleged herein, and permanently enjoining

Defendants from continuing to engage in such unlawful acts and practices;

109. Requiring Defendants to pay civil penalties pursuant to Neb. Rev. Stat. §§ 59-1614 and 87-303.11, and pay direct economic damages for each affected Nebraska resident pursuant to Neb. Rev. Stat. § 87-806;

110. Requiring Defendants to pay restitution to affected Nebraska residents pursuant to Neb. Rev. Stat. §59-1608(2) and § 87-303.05(1);

111. Requiring Defendants to pay all costs and fees for the prosecution and investigation of this action pursuant to Neb. Rev. Stat. §§ 59-1608 and 87-303(b);

112. Enjoining Defendants from committing or continuing to commit further deceptive or unconscionable trade practices pursuant to Neb. Rev. Stat. § 87-303.05(1); and

113. Enjoining Defendants from committing or continuing to commit further unfair or deceptive acts or practices pursuant to Neb. Rev. Stat. § 59-1608(1); and.

114. Granting any such further relief as the Court may deem appropriate.

JURY DEMAND

The State demands a trial by jury on all issues so triable.

DATED: December 16, 2024

MICHAEL T. HILGERS, #24483
Nebraska Attorney General

BY: /s/ Tyrone E. Fahie
Tyrone E. Fahie, #28125
Beatrice O. Strnad, #28045
Justin C. McCully, #27067
Consumer Protection Bureau
Office of the Attorney General
2115 State Capitol
Lincoln, NE 68509-8920
Phone: (402) 471-2811
tyrone.fahie@nebraska.gov
bebe.strnad@nebraska.gov
justin.mccully@nebraska.gov

William A. Burck
Adam B. Wolfson
Jennifer J. Barrett
Derek L. Shaffer
Sara C. Clark
Ryan Swindall
Quinn Emanuel Urquhart & Sullivan,
LLP
865 S. Figueroa St., 10th Floor
Los Angeles, California 90017
Phone: (213) 443-3000
williamburck@quinnemanuel.com
adamwolfson@quinnemanuel.com
jenniferbarrett@quinnemanuel.com
derekshaffer@quinnemanuel.com
saraclark@quinnemanuel.com
ryanswindall@quinnemanuel.com

Attorneys for the State of Nebraska