

In the Iowa District Court for Polk County

STATE OF IOWA, *ex rel.* BRENN
BIRD, ATTORNEY GENERAL

Plaintiff,

v.

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

Defendants.

Case No. _____

PETITION

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. PARTIES	3
III. JURISDICTION AND VENUE	4
IV. FACTUAL ALLEGATIONS.....	5
A. Defendants Process and Store Iowa Consumers’ Personal Information.....	5
B. Hackers Access Change’s Systems and Exfiltrate Sensitive Data.....	9
C. Change and UHG Finally Learn of the Attack	11
D. Change’s Security Flaws.....	12
E. Failure to Provide Notice	15
F. The Data Breach Upends the Healthcare System and Places Iowans at Risk.....	17
G. Injunctive Relief Is Essential to Address The Ongoing Harms Caused By Defendants	20
V. CLAIMS FOR RELIEF	21
A. Violations of the CFA (Iowa Code § 714.16 <i>et seq.</i>).....	21
B. Violation of the PISBPA (Iowa Code § 715C <i>et seq.</i>).....	25
VI. CONCLUSION AND PRAYER	26

I. INTRODUCTION

1. This action concerns a data breach that exposed personal information and electronic protected health information of 192.7 million Americans—including approximately 2.2 million Iowans¹—and halted critical operations of scores of Iowa healthcare providers. Both before and after the breach, Defendants Change Healthcare Inc. (“Change”), UnitedHealth Group Incorporated (“UHG”), and Optum, Inc. (“Optum”) made material representations about their cybersecurity practices and systems that were responsible for keeping Iowans’ data safe. Those representations were false. The result was one of the largest data breaches in American history.

2. 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 Iowa alone, Change processes more than one million 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.

3. 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.”

¹ In an April 2025 letter to the Iowa Attorney General, Change stated that it had sent 2,193,253 individual notice letters to addresses in Iowa. In June 2025, Change revised that estimate to 2,165,340 Iowa addresses.

² In 2023, Defendants processed at least 124 million claims. *See The Optum 2024 Revenue Cycle Denials Index*, Optum, 4, <https://business.optum.com/en/insights/denials-index.html>. Assuming a proportional number of claims processed in Iowa yields over a million claims per year.

4. 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.

5. In reality, what UHG tried to describe as a relatively benign “isolat[ion]” of Change’s systems was one of the largest data breaches in American history. It caused a total shutdown of the Change platform. The 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.

6. The breach occurred because Change’s systems were insecure, outdated, and lacked appropriate segmentation and redundancies—in violation of Change’s advertised practices, company policies, federal privacy requirements, and basic standards of enterprise information security.

7. Following the breach, UHG disabled Change’s processing services entirely. This disabling blocked countless transactions from the end of February through the middle of March, crippling Iowan healthcare providers and their care of affected Iowans. 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 and asking for patients’ financial information.

8. Healthcare 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% of those hospitals reported direct impacts to patient care, while 94% reported adverse financial impact.

9. 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 Iowa residents and healthcare providers, and the harm suffered by Iowans—began to come to light. It became clear that Defendants materially misrepresented the quality and characteristics of their cybersecurity systems to Iowans and to Iowa healthcare providers, in violation of Iowa law.

10. In further contravention of Iowa 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.

11. It was not until July 31, 2025, one year later, that Change updated the total estimated number of individuals affected to 192.7 million. As of August 2025, Defendants had yet to mail final breach notification letters to state attorneys general confirming the number of individuals affected in each state. And Change was still notifying affected individuals as of October 2025—*twenty months* after their data was compromised.

12. Plaintiff State of Iowa, *ex rel.* Brenna Bird, Attorney General of Iowa (“Attorney General,” “State of Iowa,” or “State”) brings this action to vindicate the rights of Iowa citizens and protect their most sensitive personal, medical, and financial information in accordance with the Iowa Consumer Fraud Act, Iowa Code § 714.16 *et seq.* (“CFA”) and the Personal Information Security Breach Protection Act, Iowa Code § 715C *et seq.* (“PISBPA”).

II. PARTIES

13. Plaintiff is the State of Iowa, *ex rel.* Brenna Bird, Attorney General. The State, by and through its Attorney General, brings this action as the chief law enforcement officer of the state of Iowa charged, *inter alia*, with civil enforcement of the CFA and the PISBPA. Iowa Code §§ 714.16(7), 715C.2(9); 13.2. The Attorney

General brings this action on behalf of the people of the State of Iowa to protect the state and its residents from Defendants' unlawful business practices.

14. Defendant Change Healthcare Inc. is incorporated in Delaware with its principal place of business in Minnesota. It became a subsidiary of UHG in 2022 and is operated by Optum, another UHG subsidiary. It provides services for numerous hospitals and healthcare systems throughout Iowa, 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 Iowa residents.

15. Defendant Optum, Inc. maintains its principal place of business in Minnesota and is incorporated in Delaware. It regularly transacts business in Iowa 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.

16. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in 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 Iowa residents and entities.

III. JURISDICTION AND VENUE

17. At all times relevant to this Petition, Defendants engaged in substantial activities affecting consumers in Iowa insofar as they provided healthcare clearinghouse and related services to healthcare providers and consumers in Iowa. Defendants were also in possession and/or had control over sensitive personal information of Iowa residents.

18. This Court has personal jurisdiction over Defendants because the conduct and injuries from which the Petition arose took place in Iowa, harmed Iowans, and specifically targeted Iowans.

19. This Court has jurisdiction over the subject matter of this action under Iowa Code §§ 714.16(7) and 714.16(10). Polk County is a proper venue because it is a “county where the transaction or any substantial part of the transaction occurred” and because it is “where one or more of the victims reside.” Iowa Code § 714.16(10).

20. The Attorney General, as Iowa’s Chief Law Enforcement Officer, is expressly authorized to enforce the CFA and the PISBPA. Iowa Code §§ 714.16(7), 715C.2(9).

21. Beyond her express statutory authority, the Attorney General has standing to bring a legal action in the name of the State when the interest of the state requires such an action. *See* Iowa Code § 13.2.

IV. FACTUAL ALLEGATIONS

A. Defendants Process and Store Iowa Consumers’ Personal Information

22. 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 100 million medical claims each year.

23. In the course of its business, Change receives, processes, and stores electronic protected health information of over 100 million Americans, including more than one million Iowans. This includes statutorily protected information, such as Iowans’ Social Security numbers, driver’s license numbers, and financial account numbers. *See* Iowa Code § 715C.1(11)(a).

24. Change functions as a supplier providing services directly connected to consumer healthcare transactions. When a consumer purchases health insurance from a health insurer, or receives healthcare services from a provider, or purchases prescription drugs from a pharmacy, Change supplies essential verification and payment processing services that are integral components of these transactions. Change has boasted that its services directly affect consumers, advertising that its “solutions streamline the engagement, care, and payment experience to improve the patient journey.” Change has also touted the quality of its cybersecurity systems, including in its Code of Conduct and Global Privacy Notice.

25. Because Change advertises and sells its services on the basis of these representations, the information Change receives, processes, and stores is subject to the requirements of the CFA, which prohibits advertising services to have certain characteristics or benefits when in fact they do not. Iowa Code § 714.16(2)(a).

Further, Change’s failure to meet basic data security standards is also a violation of the minimum standards set forth in 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”). *See* HIPAA, 45 CFR Part 160 and Subparts A and C of Part 164.

26. As one of the largest processors of sensitive health information in the nation, Change, its parent entity UHG (which sees revenues more than \$440 billion annually—more than 40 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.

27. 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.

28. For example, at the time of the breach, Defendants had a policy requiring Multi-Factor Authentication (“MFA”) on all user authenticated systems before an employee (or non-employee) accessed protected or confidential information.

29. Defendants also had a policy that required [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] That policy further required that [REDACTED]
[REDACTED]
[REDACTED]

30. Yet another Defendant policy mandated that [REDACTED]

[REDACTED] and
that [REDACTED]

31. Defendants also required that [REDACTED]
[REDACTED]
[REDACTED]

32. Defendants’ public representations also represented that they recognized the importance of proper data handling and utilized up-to-date security systems. These misleading and deceptive public statements and advertisements were intended to induce—and did induce—healthcare providers and healthcare industry participants to transact with Change.

33. 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.”

34. 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 as 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.”

35. That Global Privacy Notice also provided 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.

36. 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.”

37. Indeed, Change had 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.”

38. Another arm of Change’s website boasted 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

39. 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 a Telegram group chat that advertises the sale of stolen credentials.

40. 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.

41. 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.

42. That unauthorized 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.

43. From there, the hacker created privileged accounts with administrator capabilities that permitted access to and deletion of all files, changes to system configurations, and similar administrator-level activities. Those actions went to the heart of the integrity of Change's most critical IT infrastructure, but still went undetected by Defendants.

44. 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 several "backdoors" that would allow the hacker to return to those environments if Change detected the suspicious activity and try to block access.

45. 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 2.2 million Iowans. Exfiltrated information included Social Security numbers, driver's license numbers, 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.

46. Ironically, on February 13, 2024—the day after the hackers infiltrated Change’s systems—Defendants held an Executive Steering Committee meeting. The Executive Summary of that meeting stated that [REDACTED]

C. Change and UHG Finally Learn of the Attack

47. 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.

48. That day, in response, Defendants took Change’s systems offline. In other words, 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.

49. 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.

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

51. Paying the ransom did not bring Change’s systems back online or mitigate the harm. Because Change was unable to check every system and interface for backdoors, and because Change’s backup systems were also compromised, Change could not 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.

52. Notwithstanding the ransom payment, the data of approximately 2.2 million Iowans 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 its cut of Change's \$22 million payment.

D. Change's Security Flaws

53. All the harm these attacks caused was 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.

54. 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. The physical servers Change used were less secure and lacked appropriate segmentation to take into account the sensitivity of the data at issue.

55. Among the outdated features of Change's systems was the lack of MFA, a commonplace, basic security feature that requires a user to provide multiple, independent pieces of evidence to authenticate their identity 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.

56. 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. Defendants should have had a multi-level backup system (day, week, month) in place.

57. And Change’s redundancies were also affected, inadequate, or both. Redundancy systems are designed to keep multiple independent copies of critical components so that the failure of one system does not stop operations. For example, a company might use multiple cloud services to store data—a primary service that handles live traffic and a secondary service that stores backup copies. But when the cyberattack occurred, many of Defendants’ redundancy systems were not sufficiently segregated from the rest of the company’s infrastructure, while others were in the process of being upgraded, potentially leaving them inactive or vulnerable to the cyberattack. This prevented the backup and redundancy systems from being effectively utilized to mitigate the damage from the breach.

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

59. Defendants’ security lapses were far more ubiquitous and egregious than initially disclosed to the public, violating the most basic and obvious network security standards. Such failures include:

(a) The absence of MFA throughout Change’s most sensitive systems and networks;

(b) Inadequate measures to block or detect simple network enumeration techniques, including lack of proper segmentation across Defendants’ systems, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED];

(c) Inadequate measures to block simple privilege escalation techniques, including [REDACTED]

(d) [REDACTED]

(e) [REDACTED]

(f) [REDACTED]

(g) [REDACTED]

(h) [REDACTED]

(i) [REDACTED]

(j) The use of legacy systems, some of which were up to 40 years old;

(k) Insufficient use of backup and redundancy systems; and

(l) Other failures.

60. Along with violating its own stated policies and HIPAA, which is itself sufficient to show that Change’s systems fell far below their advertised standards, Defendants’ egregious and ubiquitous security lapses contravened widely adopted cybersecurity frameworks.

61. By way of example, the National Institute of Standards and Technology (“NIST”) emphasizes that “[p]asswords alone are not effective in securing your most sensitive business assets, as they have become too easy for threat actors to access.”

NIST further states that “[e]nabling MFA on all accounts that offer it is essential for reducing the cybersecurity risks.” Accordingly, NIST’s widely adopted cybersecurity framework, “Security and Privacy Controls for Information Systems and Organizations,” recommends implementing MFA controls for both privileged and non-privileged accounts. Similarly, the Center for Internet Security’s Critical Security Controls advises requiring MFA for externally exposed applications and remote network access. Additionally, Citrix—the platform exploited by hackers to breach Change’s systems—warns that “[i]t’s critical . . . to also implement multi-factor authentication as a backup in case passwords do become compromised.”

62. Change’s failure to implement these widely recognized security controls—despite having written policies acknowledging the necessity of such measures and external representations claiming compliance—demonstrates a conscious disregard for established security obligations, not merely suboptimal security practices.

E. Failure to Provide Notice

63. Defendants are and have been aware of what data was compromised, and they know consumers’ information remains accessible on the dark web. Yet, simple notices to consumers of the breach have still not been provided.

64. Such a delay—for many Iowa consumers, a delay of *nearly two years*—is patently unreasonable. The cybercriminals gained access to the data on roughly February 11, 2024, and Change became aware of the breach when ransomware was deployed on February 21. By March 3, 2024, Change had already paid a \$22 million ransom and received detailed information about the scope and nature of the breach, including specific information about what data had been exfiltrated. And since learning of the breach, Change has, by its own account, over 100 data scientists analyzing the breach, purportedly working 24 hours-a-day, seven days-a-week.

65. Yet, as late as July 2024, Defendants had still not notified consumers that their data might have been compromised. Half a year later, in December 2024, Change still had not provided notice to every individual affected by the breach, continuing to claim that it was in the “final stages” or the notification process. And in October 2025, Change was still mailing notices to affected individuals—*ten* months after it was purportedly in the “final stages” of notification, and over *twenty* months after the attack occurred. This delay left citizens more vulnerable to exploitation of the sensitive personal financial, health, and identifying information.

66. Defendants’ notification delays are all the more unreasonable because they possess affected Iowa consumers’ and commercial entities’ emails, thus rendering any delay in notification unreasonable. It is evident that Defendants possess these emails: the hackers explicitly stated that emails were exfiltrated during the breach, and Change has publicly confirmed their exposure. Following the \$22 million ransom payment, Defendants regained access to the exfiltrated personally identifiable information, including emails. Thus, even assuming Defendants temporarily lost possession of affected email addresses, they have possessed them since March 2024.

67. Nor have Defendants made a “[c]onspicuous posting of the notice” on their website. The notices on Defendants’ respective homepages were either non-conspicuous (UHG) or non-existent (Optum). Furthermore, the notices were posted far too late—certainly not “in the most expeditious manner possible and without unreasonable delay.”

68. Defendants’ delays extend far beyond what is reasonable, even for a complex breach, particularly given:

- (a) Defendants’ significant resources, including access to “over 100 data scientists analyzing the breach” working “24 hours-a-day, seven days-a-week,” as Defendants claim;

(b) The critically sensitive nature of the compromised data, which increases the urgency of notification to allow affected individuals to take protective measures;

(c) Defendants' experience in healthcare data management, which should afford them the capability to efficiently analyze affected data; and

(d) Defendants' statutory obligations, of which they have been on notice, including under Iowa Code § 715C.2(1), which requires notice to be "made in the most expeditious manner possible and without unreasonable delay."

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

69. Defendants' conduct caused direct and significant economic harm to Iowans and Iowa 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 Iowa healthcare system.

70. 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.

71. 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.

72. Most hospitals polled by the American Hospital Association reported financial and/or operational impacts because of the cyberattack.³ 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.

73. Those that stuck with Change faced substantial cash flow shortages as they could not receive payments from claims (or even submit new claims). One third of hospitals reported that more than half of their revenue was disrupted as a result of the cyberattack.⁴ Many were forced to pull from reserves, take out private loans to pay healthcare providers and acquire medicine and supplies, or rely on cash advances to stay afloat. At least one hospital cashed out investments and certificates of deposits to maintain operations—losing out on interest and investment income.

74. Those that switched clearinghouses from Change also faced cash flow problems, beyond the time and resources spent converting to a new provider. Some hospitals were forced to hire consultants or other third parties to facilitate their transition to new claims processors.

75. 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.

³ *Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field*, American Hospital Association, <https://perma.cc/N4HU-LYBE>.

⁴ *Id.*

76. Those harms to providers flowed directly to Iowan patients, whose most sensitive personal information—which itself has value—has been stolen. Iowans 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.

77. Although Change’s systems have largely been restored, Iowans 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.

78. 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.

79. The full scope and magnitude of the harm suffered by Iowans is still coming to light, but what has already manifested is both widespread and significant.

G. Injunctive Relief Is Essential to Address The Ongoing Harms Caused By Defendants

80. Injunctive relief is necessary and appropriate under the CFA, which permits the State to seek injunction if a person "has engaged in, is engaging in, or is about to engage in a practice declared to be unlawful[.]" Iowa Code § 714.16(7). Such injunctive relief is warranted here.

81. First, upon information and belief, Defendants have yet to notify many Iowan consumers of the compromise of their financial, health, and personal identifying information, thus failing to fulfil their obligation to notify Iowans.

82. Nor have Defendants given verifiable assurances that their rebuilt systems have remediated Change's widespread and egregious security inadequacies.

Given Defendants' past deceptive conduct, the State has no reason to believe that Defendants' unfair and deceptive practices have ceased. Because Defendants continue to do sell and advertise their services in Iowa, and continue to process millions of Iowans' data, injunctive relief is warranted.

83. Without injunctive relief, Iowa faces a substantial risk of:

(a) Continued non-compliance with notification requirements, leaving affected Iowans unable to take necessary measures to protect themselves from identity theft and fraud;

(b) Persistent security vulnerabilities that risk additional data breaches exposing Iowa consumers' most sensitive personal and medical information and further service disruptions that could again impair Iowans' access to critical healthcare services; and

(c) Ongoing violations of Iowa law causing irreparable harm to Iowa consumers and healthcare providers.

V. CLAIMS FOR RELIEF

A. Violations of the CFA (Iowa Code § 714.16 *et seq.*)

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

85. Section 2(a) of the CFA states as follows:

The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for

charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice. It is deceptive advertising within the meaning of this section for a person to represent in connection with the lease, sale, or advertisement of any merchandise that the advertised merchandise has certain performance characteristics, accessories, uses, or benefits or that certain services are performed on behalf of clients or customers or that person if, at the time of the representation, no reasonable basis for the claim existed. The burden is on the person making the representation to demonstrate that a reasonable basis for the claim existed.

Iowa Code § 714.16(2)(a).

86. The CFA defines “Merchandise” as “any objects, wares, goods, commodities, intangibles, securities, bonds, debentures, stocks, real estate or services.” *Id.* § 714.16(1)(e). “Sale” is defined as “any sale, offer for sale, or attempt to sell any merchandise for cash or on credit.” *Id.* § 714.16(1)(g). And “advertisement” is defined to “include[] the attempt by publication, dissemination, solicitation, or circulation to induce directly or indirectly any person to enter into any obligation or acquire any title or interest in any merchandise.” *Id.* § 714.16(1)(a). Defendants sell and advertise merchandise as defined by the CFA.

87. Defendants’ advertisements and representations, many—but not all—of which are identified in this Petition, 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 the CFA. For example, contrary to their own well-publicized policies, procedures, and public representations, Defendants:

- (a) Represented that Change would store and protect electronic protected health information and personal identifying information “by following [Change’s] privacy, security, and data information protection policies,” when in fact they did not;
- (b) 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 in fact did not;
- (c) 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 [Change’s] internal networks and systems,” but in fact did not;
- (d) 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;
- (e) Represented that their services had certain privacy and security characteristics and benefits that the services did not have;
- (f) Represented that their services were of a particular standard and quality with respect to privacy and security features when they were not; and

- (g) Otherwise made false or misleading statements in a privacy policy, published on the Internet or otherwise distributed or published, in connection with the sale or advertisement of merchandise.

88. Defendants thus violated the CFA by engaging in false, misleading, and deceptive conduct and unfair practices in the sale and advertisement of their services in Iowa. Upon information and belief, Defendants' at-issue practices are ongoing.

89. The Attorney General is statutorily authorized to bring a civil action under the CFA. Iowa Code § 714.16(7).

90. The State can recover civil penalties of up to \$40,000 for every violation of the CFA. *Id.* Here, Defendants' violated the CFA by engaging in deceptive acts or practices that were directed to each Iowa resident for whom Change possessed data and to each entity which transacted with Change using Iowans' personal, financial, or health information. Accordingly, each transaction that Change processed involving the personal, financial, or health information of an Iowa resident or involving an Iowa entity; each Iowa resident's personal, financial, or health information that Change possessed and was affected by the breach; and each transaction that an Iowa entity would have processed but could not process because of the shutdown of Change's system constitutes a separate violation of the statute.

91. The State can also recover civil penalties of up to \$5,000 for every violation of the CFA committed against an older individual, defined as any individual who is sixty years of age or older. Iowa Code §§ 714.16A(1), 714.16A(3). Here, Defendants knew or should have known that older individuals were substantially more vulnerable to their conduct because Defendants possessed sensitive medical information that would have shown those individuals' age, poor health, and infirmity—the very same information that was lost in the data breach. These factors weigh in favor of civil penalties under the CFA. *See* Iowa Code § 714.16A(2).

92. The CFA also authorizes the court to “restore to any person in interest any moneys or property, real or personal, which have been acquired by means of a practice declared to be unlawful by this section[.]” *Id.* Where, as here, “the cost of administering reimbursement outweighs the benefit to consumers . . . the court may order disgorgement of moneys or property acquired by the person by the person awarding the moneys or property to the state to be used by the attorney general for the administration and implementation of” the CFA. *Id.*

B. Violation of the PISBPA (Iowa Code § 715C *et seq.*)

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

94. The Personal Information Security Breach Protection Act (“PISBPA”), Iowa Code § 715C, requires any person that owns or licenses data that includes a consumer’s personal information to make notification of any data breach “in the most expeditious manner possible and without unreasonable delay[.]” Iowa Code § 715C.2(1).

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

96. Defendants waited until July 2024, at the earliest, to *begin* to send Iowa consumers direct written or electronic notice of the breach, as is required by the statute. Iowa Code § 715C.2(4). In July 2025, over a year later, Defendants had still not completed the process of notifying Iowa consumers and were still sending notifications as late as October 2025.

97. 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.

98. Nor was the “substitute notice” provision, which requires notice by email, conspicuous posting, or notification to major statewide media, timely satisfied.

See Iowa Code § 715C.2(4)(c). As a result, upon information and belief, Defendants' violations are ongoing.

99. Defendants' delay in notifying Iowa consumers was unreasonable in violation of the statute, and each such failure is its own violation of the statute.

100. Violation of the PISBPA is considered a violation of the CFA, and the Attorney General is entitled to all the remedies available under the CFA. Iowa Code § 715C.2(9)(a). Such remedies include civil penalties of up to \$40,000 for each violation. Iowa Code § 714.16(7). Additionally, the PISBPA entitles the Attorney General to "seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation." Iowa Code § 715C.2(9)(a).

VI. CONCLUSION AND PRAYER

WHEREFORE, the State of Iowa, *ex rel.* Attorney General Brenna Bird respectfully requests that this Court enter judgment against Defendants and:

- A.** Declare that Defendants violated the Iowa Consumer Fraud Act, Iowa Code § 714.16 *et seq.* and the Personal Information Security Breach Protection Act, Iowa Code § 715C *et seq.*, by engaging in the unlawful acts and practices alleged herein;
- B.** Award the State civil penalties of \$40,000 per violation pursuant to Iowa Code § 714.16(7);
- C.** Award the State civil penalties of \$5,000 for each violation of the CFA committed against an older individual pursuant to Iowa Code § 714.16A(1).
- D.** Require Defendants to disgorge to the Attorney General all moneys or property acquired in violation of the Iowa Consumer Fraud Act pursuant to Iowa Code § 714.16(7);

- E. Award the State damages on behalf of persons injured because of Defendants' violation of the Personal Information Security Breach Protection Act pursuant to Iowa Code § 715C.2(9);
- F. Enjoin Defendants from committing or continuing to commit further unlawful practices pursuant to Iowa Code § 714.16(7);
- G. Require Defendants to pay all costs and fees for the prosecution and investigation of this action pursuant to Iowa Code § 714.16(11); and
- H. Grant any such further relief as the Court may deem appropriate.

DATED: March 31, 2026

BRENNA BIRD
Iowa Attorney General

BY: /s/ William R. Pearson
William R. Pearson (AT0012070)
Assistant Attorney General
Daniel L. Barnes (AT0015826)
Deputy Attorney General for Consumer Protection
1305 E. Walnut St.
Des Moines, Iowa 50319
(515) 242-6773
william.pearson@ag.iowa.gov
daniel.barnes@ag.iowa.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 Iowa

* Applications for admission *pro hac vice*
forthcoming