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.	Case No. CI 24-4356 **ORDER ON MOTION TO DISMISS**

This case was before the Court on June 18, 2025, for a hearing on Defendants' Motion to Dismiss (Filing No. 18). Tyrone Fahie, Adam Wolfson, and Johnston Hill appeared for Plaintiff State of Nebraska, ex rel. Michael T. Hilgers, Attorney General ("State"). Timothy Engler and Allison Ryan appeared for Defendants Change Healthcare Inc. ("Change"), UnitedHealth Group Incorporated ("UHG"), and Optum, Inc. ("Optum") (collectively "Defendants"). Defendants sought judicial notice of publications on UHG's website, cited on pages 4 and 14 of the opening brief. The State had no objection and judicial notice was taken. The Court heard arguments and took the motion under advisement. Now being duly advised, the Court finds the motion should be overruled.

BACKGROUND

For this pending motion to dismiss, the Court accepts as true the following allegations in the Amended Complaint:

1. 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 and millions of claims per year in Nebraska alone. UHG acquired Change in 2022 and

had control over Change's IT operations and systems at all relevant times. Change is operated by Optum. (Am. Comp. ¶ 1.)

2. 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. In the course of its business, Change receives, processes, transmits, and stores sensitive personal, medical, and financial information, as well as electronic protected health information, of tens of millions of Americans, including nearly a million Nebraskans. 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 prescription drugs from a pharmacy, Change supplies essential verification and payment processing services that are integral to 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." (*Id.* at ¶¶ 13, 22-24.)

3. Information Change receives, processes, and stores is subject to Nebraska law and the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("HIPAA"). (*Id.* at ¶ 25.)

4. When UHG acquired Change in 2022, both were aware that Change maintained outdated and highly vulnerable systems. Among the outdated features was the lack of multi-factor authentication ("MFA"), in violation of UHG's own stated policies. (*Id.* at ¶¶ 54-55.)

5. In February 2024, Change's systems were compromised in a cyberattack. On February 11, 2024, the username and password for a low-level employee's access to Change's systems were posted in a Telegram group chat. Using those credentials, a hacker gained

entry to the systems, created accounts with administrator capabilities, and then navigated through the systems, installing applications, malware, and "backdoors" that would allow reentry if Change detected their activity and tried to block access. The hacker exfiltrated personal identifying information, financial account information, and protected health information of tens of millions of individuals, including nearly 900,000 Nebraskans. Defendants did not become aware of this cyberattack until February 21, 2024, when the hacker deployed ransomware, causing outages and disruptions. (*Id.* at ¶¶ 39-47.)

6. In response to the cyberattack, Defendants took Change's systems offline. Because Change was unable to check every system for backdoors and because its backup systems were also compromised, Change could not repair its systems; instead, it opted to rebuild them from the ground up. Change's inadequate redundancy systems caused additional delay and harm to providers, payers, and consumers. Despite a ransom payment, the data of approximately 900,000 Nebraskans remained in the hands of the hackers, and they still leaked files of stolen data. (*Id.* at ¶¶ 48, 51-52.)

7. Defendants play such a critical role in healthcare services that when their systems failed, consumers were unable to fill prescriptions, verify insurance coverage, or access essential benefits. (*Id.* at ¶ 112.) Even after the systems have largely been restored, Nebraskans are still incurring and are likely to incur direct economic damages from Defendants' conduct. The full scope and magnitude of the harm suffered by Nebraskans is still coming to light but has been manifested as both widespread and significant. (*Id.* at ¶¶ 80-82.)

8. At the time of the cyberattack, Defendants had numerous policies requiring MFA on all user authenticated systems, regular backups, weekly vulnerability scans, a separate backup zone with physical or logical separation, etc. (*Id.* at ¶¶ 27-31.)

9. Defendants made extensive public representations about their data security practices, including representations that they "exercise care and discretion when handling [restricted and confidential] information," "regularly monitor [their] systems," and store electronic protected health information in a manner that "meets or exceeds HIPAA Privacy and Security Rule requirements." (*Id.* at ¶¶ 32-34, 36.)

10. Despite these policies and representations, Defendants' security practices included the lack of MFA throughout their systems, inadequate measures to block or detect network enumeration techniques, inadequate measures to block privilege escalation techniques, widespread password reuse across domains, storage of passwords in plain and clear text, granting unnecessary access to users in violation of the principle of least privilege, and inadequate training, supervision, and monitoring. (*Id.* at ¶ 58.)

11. Defendants' security failures violated their own stated policies, advertised standards, HIPAA requirements, and widely adopted cybersecurity frameworks, such as NIST standards. (*Id.* at ¶¶ 59-60.)

12. Defendants became aware of the cyberattack on February 21, 2024. By March 3, 2024, Defendants had received detailed information about the scope and nature of the data breach. (*Id.* at ¶¶ 47, 62-63.)

13. Despite being aware of the breach for months, Defendants did not begin issuing written notices to Nebraska residents until July 2024, after Change received a civil investigative demand from the Attorney General. As of December 2024, the notification process remained incomplete, and Defendants had not made a conspicuous posting of the notice on their website without unreasonable delay. (*Id.* at ¶¶ 64-67.)

14. Defendants' data security failures, improper breach notifications, and misrepresentations are ongoing and have impacted the public interest. (*Id*. at ¶¶ 83-85, 90, 92, 96, 98, 105, 113, 114, 120.)

In the Amended Complaint, the State brings five claims against Defendants for alleged violations of the Nebraska Consumer Protection Act ("CPA"), Neb. Rev. Stat. § 59-1601 *et seq.*; the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 ("Reasonable Security Statute" or "RSS"), Neb. Rev. Stat. § 87-801, *et seq.*; and the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Neb. Rev. Stat. § 87-301 *et seq*. The State seeks to permanently enjoin Defendants from continuing to engage in the alleged unlawful acts and practices. The State also requests civil penalties under §§ 59-1614 and 87-303.11, direct economic damages under § 87-806, restitution under §§ 59-1608(2) and 87-303.05(1), costs and fees, and any further relief as the Court may seem appropriate. In Filing No. 18, Defendants move the Court to dismiss each count in the Amended Complaint for failure to state a claim under Neb. Ct. R. Pldg. § 6-1112(b)(6).

STANDARD OF REVIEW

For purposes of a motion to dismiss pursuant to § 6-1112(b)(6), a court generally must ignore materials outside the pleadings but may consider some materials that are part of the public record, as well as materials necessarily embraced by the pleadings. *Nadeem v. State*, 298 Neb. 329, 334, 904 N.W.2d 244 (2017). An affirmative defense may be asserted in a § 6-1112(b)(6) motion if it appears on the face of the complaint. *Schaeffer v. Frakes*, 313 Neb. 337, 346, 984 N.W.2d 290, 298-99 (2023). When reviewing a motion to dismiss under § 6-1112(b)(6), a court accepts as true all well-pled facts in the complaint and draws all reasonable inferences in favor of the plaintiff. *Vasquez v. CHI Properties, LLC*, 302 Neb. 742, 749, 925 N.W.2d 304, 313 (2019).

Nebraska is a notice pleading jurisdiction. *Id.* at 750, 925 N.W.2d at 313. Civil actions are controlled by a liberal pleading regime; a party is only required to set forth a short and plain statement of the claim showing that the pleader is entitled to relief and is not required to plead legal theories or cite appropriate statutes so long as the pleading gives fair notice of the claims asserted. *Id.* To prevail against a motion to dismiss under § 6-1112(b)(6), a plaintiff must allege sufficient facts, accepted as true, to state a claim to relief that is plausible on its face. *Id.* at 759, 925 N.W.2d at 318. If a plaintiff does not or cannot allege specific facts showing a necessary element, the factual allegations, taken as true, are nonetheless plausible if they suggest the existence of the element and raise a reasonable expectation that discovery will reveal evidence of the element or claim. *Id.* at 759, 925 N.W.2d at 318-19. Dismissal under § 6-1112(b)(6) should be granted only in the unusual case where a plaintiff includes allegations that show on the face of the complaint that there is some insuperable bar to relief. *Id.* at 750, 925 N.W.2d at 313. One of multiple remedies pleaded within the context of a single cause of action is not the proper subject of dismissal under § 6-1112(b)(6) for failure to "state a claim." *Id.* at 759-60, 925 N.W.2d at 319.

ANALYSIS

I. CPA Claims – Unfair and Deceptive Acts or Practices (Counts 1 and 2)

The CPA claims are brought under Neb. Rev. Stat. § 59-1602, which outlaws "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Count 1 alleges that Defendants have engaged in unfair acts or practices by failing to implement and maintain reasonable security practices, in violation of Neb. Rev. Stat. § 87-808 of the Reasonable Security Statute. Count 2 alleges that Defendants have engaged in deceptive acts or practices by making misrepresentations regarding data security and by failing to notify affected consumers and entities of the data breach in a timely manner. Under § 87-806(2), "[a]

violation of section 87-808 shall be considered a violation of section 59-1602 and be subject to the Consumer Protection Act and any other law which provides for the implementation and enforcement of section 59-1602." Section 87-808(1) of the RSS provides:

> To protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure, an individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska shall implement and maintain reasonable security procedures and 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, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information.

Defendants move the Court to dismiss both causes of action under the CPA, arguing that (1) the State has failed to allege any unfair or deceptive acts or practices under a heightened pleading standard; (2) an unreasonable data security practice in violation of § 87-808, unless unfair or deceptive, does not automatically violate § 59-1602; (3) the claims fall under the regulatory exemption to the CPA; and (4) the State has failed to state a CPA claim because it is not entitled to any relief available under the CPA. The Court rejects these arguments.

A. <u>The State has adequately alleged unreasonable, unfair, and deceptive conduct.</u>

Defendants assert that the State has failed to allege sufficient facts to state Defendants' conduct at issue is unfair and not merely unreasonable. Defendants also argue that the State has not pleaded facts with particularity to allege any deceptive conduct. The parties disagree as to whether an unreasonable data security practice under the RSS must be either unfair or deceptive to violate the CPA, and whether a heightened pleading standard applies to CPA claims alleging deceptive conduct. The Court need not resolve these disagreements here. Accepting all well-pled facts as true and drawing all reasonable inferences in favor of the State, the Court finds that the Amended Complaint contains extensive factual allegations to show both unreasonableness and

unfairness in Defendants' data security practices. The Court further finds that the State has adequately pleaded deceptive conduct with particularity. Thus, the Court rejects Defendants' contention that the State has failed to sufficiently allege unfair or deceptive conduct.

B. The State has sufficiently stated CPA claims not subject to the regulatory exemption.

Defendants argue that the alleged violations of § 87-808 are also regulated by federal law, rendering the CPA claims subject to the regulatory exemption of the CPA. Under the plain text of § 87-806(2), a violation of § 87-808 is subject to the CPA, which includes its regulatory exemption. Neb. Rev. Stat. § 59-1617(1) provides, in relevant part, that "the Consumer Protection Act shall not apply to *actions or transactions* otherwise permitted, prohibited, or regulated under laws administered by . . . any other regulatory body or officer acting under statutory authority of this state or the United States." (Emphasis supplied.)

This provision of the CPA was first interpreted by the Nebraska Supreme Court in *Kuntzelman v. Avco Financial Services, Inc.*, 206 Neb. 130, 132-33, 291 N.W.2d 705, 706 (1980). There, the Nebraska Supreme Court concluded that the exemption excluded from the purview of the Consumer Protection Act a loan made pursuant to the installment loan act by an entity licensed thereunder to make such a loan. In so doing, the Court emphasized that not only was the licensee regulated by the state, but the very act of making the loan was regulated. *Id.* at 135, 291 N.W.2d at 707. "If a particular practice found to be unfair or deceptive is not regulated, even though the business is regulated generally, it would appear to be the legislative intent that the provisions of the act should apply." *Id.* at 134-35, 291 N.W.2d at 707 (quoting *Dick v. Attorney General*, 83 Wash. 2d 684, 688, 521 P.2d 702, 705 (1974)). In other words, even if an entity operates in a sector subject to federal regulations, the regulatory exemption applies only if the challenged action or transaction is regulated by a state or federal authority. See *Wrede v.*

Exch. Bank, 247 Neb. 907, 915, 531 N.W.2d 523, 529 (1995) ("while particular conduct is not immunized from the operation of the Consumer Protection Act merely because the actor comes within the jurisdiction of some regulatory body, immunity does arise if the conduct itself is also regulated.")

Here, as alleged in paragraph 25 of the Amended Complaint, certain information Change receives, processes, and stores is subject to federal regulations. It is undisputed that Defendants are heavily regulated entities subject to HIPAA. In paragraph 89a, the State alleges thirteen data security failures of Defendants that violated the RSS, CPA, and HIPAA. Defendants contend that the fact that paragraphs 25 and 89 of the Amended Complaint allege that Defendants' conduct was federally regulated at all dooms its CPA claims. While these thirteen alleged data security failures are alleged to be regulated by HIPAA and thus appear to be exempt from the purview of the CPA, factual allegations in the State's CPA claims include practices that are not alleged to be regulated by any federal statutes or regulations. For instance, paragraph 89b of the Amended Complaint alleges sixteen security failures without referencing any federal laws or regulations. Moreover, Count 2 alleges misrepresentations of data security and unreasonably delayed breach notifications, which are not claimed to be subject to HIPAA or other regulations on the face of the Amended Complaint. Accordingly, while some challenged conduct may be federally regulated and thus exempted, the Court finds that Counts 1 and 2 have sufficiently stated CPA claims that may not fall under the regulatory exemption, and the claims thus survive a motion to dismiss on that basis.

C. <u>The State has stated CPA claims upon which relief may be granted.</u>

Defendants argue that the CPA claims should be dismissed because the Attorney General is not entitled to any of the three forms of relief under the CPA, which are injunctive relief, civil

penalties, and restitution. Defendants contend that the Amended Complaint fails to allege a "real threat of future violation or a contemporary violation of a nature likely to continue or recur" for injunctive relief. Defendants further argue that the Attorney General cannot seek an injunction based on past conduct and that it is pure speculation to allege Defendants' at-issue practices are ongoing based on information and belief. However, applying the liberal pleading standard, the Court finds that the Amended Complaint has adequately alleged ongoing violations of the CPA and a risk of future harm. Accordingly, the Court rejects Defendants' argument as to injunctive relief and concludes that Counts 1 and 2 have stated CPA claims upon which relief can be granted. The Court need not address whether restitution or civil penalties are proper remedies in this Order, as remedies pleaded within a single cause of action are not subject to dismissal for failure to "state a claim." *Vasquez*, 302 Neb. at 759-60, 925 N.W.2d at 319.

II. RSS Claim – Unreasonable Notice of Security Breach (Count 3)

Neb. Rev. Stat. § 87-803 of the RSS requires, in pertinent part, that:

> (1) An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

"[T]he Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of section 87-803." Neb. Rev. Stat. § 87-806(a). Accepting the allegations in the Amended Complaint as true and drawing all reasonable inferences in favor of the State, the Court finds that the Amended Complaint contains

sufficient allegations that Defendants have failed to give notice of the security breach to affected Nebraska residents without unreasonable delay and that affected Nebraska residents suffered direct economic damages as a result. Therefore, the Court concludes that the State has adequately stated a violation of § 87-803 in Count 3.

III. UDTPA Claims – Deceptive Statements and Unconscionable Acts (Counts 4 and 5)

Count 4 alleges that Defendants have engaged in deceptive trade practices in the course of their business by making inaccurate and deceptive advertisements and representations about Change's protection of personal identifying information and electronic protected health information, as well as its compliance with regulations and industry standards, in violation of Neb. Rev. Stat. § 87-302(a)(4), (5), (8), (15) of the UDTPA, which provides:

> (a) A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, he or she:
>
> . . . .
>
> (4) Uses deceptive representations . . . in connection with goods or services;
>
> (5) Represents that goods or services have . . . characteristics . . . that they do not have[;]
>
> . . . .
>
> (8) Represents that goods or services are of a particular standard, quality, or grade . . . if they are of another;
>
> . . . .
>
> (15) Knowingly makes a false or misleading statement in privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public[.]

Count 5 alleges that Change has engaged in unconscionable acts in violation of § 87-303.01 of the UDTPA by failing to implement appropriate data security practices, making misrepresentations regarding its security practices, and failing to provide timely notification.

Defendants argue that the UDTPA claims must be dismissed because the Amended Complaint (1) fails to allege any deceptive acts or misrepresentations related to the services Change provides, (2) does not plausibly allege a risk of future harm when the UDTPA only

provides prospective relief, and (3) lacks any allegations that Defendants' at-issue conduct occurred in connection with a consumer transaction. The Court disagrees.

First, as discussed in Section I, the Court has already rejected Defendants' argument that the Amended Complaint fails to adequately allege deceptive practices or a risk of future harm. The Court also rejects the argument that the alleged practices do not relate to Change's business or trade. For the State's UDTPA claim alleging deceptive trade practices, the statutory provisions require that the alleged practices must be made "in the course of" Change's business and that deceptive representations must be "in connection with goods or services" Change provides. While Defendants argue that Change's business is healthcare clearinghouse services rather than data security, under the liberal pleading standard, the Court finds the Amended Complaint has sufficiently alleged that the at-issue conduct has occurred "in the course of" Change's business and "in connection with" the services Change provides. Lastly, the Court is not persuaded by the argument that the State has failed to plausibly allege unconscionable acts "in connection with a consumer transaction," as required by § 87-303.01(1). While Defendants contend that consumers are largely unaware of Change's role in the healthcare system and that Change primarily interacts with healthcare providers, paragraph 24 of the Amended Complaint explicitly alleges that Change functions as a supplier providing services directly connected to consumer healthcare transactions. At this stage, the Court accepts all well-pled facts as true, draws all reasonable inferences in favor of the State, and finds that the State has plausibly alleged its UDTPA claims.

CONCLUSION

Under the liberal notice pleading standard, the Court concludes that the Amended Complaint has alleged sufficient facts to state its claims under the CPA, RSS, and UDTPA.

Therefore, the Court **OVERRULES** Defendants' Motion to Dismiss (Filing No. 18) pursuant to Neb. Ct. R. Pldg. § 6-1112(b)(6).

IT IS SO ORDERED.

DATED this 10th day of November 2025.

BY THE COURT:

Susan I. Strong
District Court Judge