

**STATE OF ILLINOIS  
IN THE CIRCUIT COURT OF THE SEVENTH JUDICIAL CIRCUIT  
SANGAMON COUNTY**

**THE PEOPLE OF THE STATE OF ILLINOIS, )  
)  
Plaintiff, )  
v. )  
)  
CHS/COMMUNITY HEALTH SYSTEMS )  
INC., a Delaware corporation, and )  
CHSPSC, LLC, )  
f/k/a COMMUNITY HEALTH )  
SYSTEMS PROFESSIONAL SERVICES )  
CORPORATION, a Delaware corporation, )  
)  
Defendants. )** NO. 2020CH000162

**COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF**

NOW COMES Plaintiff, THE PEOPLE OF THE STATE OF ILLINOIS, by KWAME RAOUL, Attorney General of the State of Illinois, by Matthew W. Van Hise, Assistant Attorney General and Privacy Unit Chief, bringing this enforcement action in the public interest alleging violations of the Consumer Fraud and Deceptive Business Practices Act, 815, ILCS 505/1, *et seq.*, and the Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, in connection with a data breach disclosed by Defendants in August 2014.

Defendant CHS/Community Health Systems, Inc. (CHS/CHSI) is a Delaware publicly traded company with its principal place of business at 4000 Meridian Blvd., Franklin, TN 37067-6325 and is the parent company of Defendant CHSPSC, LLC.

Defendant CHSPSC, LLC (CHSPSC) is a Delaware limited liability company that provides management and professional services to various hospitals and other healthcare providers affiliated with CHS/CHSI. Its principal place of business is 4000 Meridian Blvd., Franklin, TN 37067.

## **PUBLIC INTEREST**

1. The Illinois Attorney General believes Defendants have engaged in and will continue to engage in the unlawful practices described below. Therefore, Plaintiff has reason to believe that Defendants have caused and will cause adverse effects to business enterprises which lawfully conduct trade and commerce in this State. Further, one of the principal purposes of this state's Personal Information Protection Act is to protect consumers from identity theft in part by requiring businesses to implement and maintain reasonable safeguards to protect personal information of consumers from unlawful use or disclosure.

2. Therefore, the State of Illinois has reason to believe that this action is in the public interest.

## **JURISDICTION & VENUE**

3. This enforcement action is brought by the Attorney General of Illinois, in the name of the State and in the public interest, pursuant to the authority granted to him by the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and the Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, and his common law authority as Attorney General to represent the People of the State of Illinois.

4. Venue for this action properly lies in Sangamon County, Illinois, pursuant to 735 ILCS 5/2-101 and 735 ILCS 5/2-201.

## **THE PARTIES**

5. Plaintiff, THE PEOPLE OF THE STATE OF ILLINOIS, by KWAME RAOUL, Attorney General of the State of Illinois, is charged, *inter alia*, with the enforcement of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and the Personal Information Protection Act, 815 ILCS 530/1, *et seq.*

6. Defendant CHS/Community Health Systems, Inc. (CHS/CHSI) is a Delaware publicly traded company with its principal place of business at 4000 Meridian Blvd., Franklin, TN 37067-6325 and is the parent company of Defendant CHSPSC, LLC.

7. Defendant CHSPSC, LLC (CHSPSC) is a Delaware limited liability company that provides management and professional services to various hospitals and other healthcare providers affiliated with CHS/CHSI. Its principal place of business is 4000 Meridian Blvd., Franklin, TN 37067.

### **TRADE & COMMERCE**

8. Subsection 1(f) of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1(f), defines “trade” and “commerce” as follows:

The terms ‘trade’ and ‘commerce’ mean the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated, and shall include any trade or commerce directly or indirectly affecting the people of this State.

### **ACTS OF AGENTS**

9. Whenever in this Petition it is alleged that Defendants did any act, it is meant that:
- A. Defendants performed or participated in the act; or
  - B. Defendants’ officers, affiliates, subsidiaries, divisions, agents or employees performed or participated in the act on behalf of and under the authority of the Defendants.

### **BACKGROUND**

10. Community Health Systems, Inc. (CHS/CHSI) and CHSPSC, LLC are headquartered at 4000 Meridian Blvd. in Franklin, Tennessee. CHSPSC provides services,

including management, consultation, and information technology services for hospitals and other affiliates of CHS/CHSI. CHS/CHSI is one of the largest publicly-traded hospital companies in the United States and a leading operator of general acute-care hospitals in non-urban and mid-size markets throughout the country.

11. Prior to the breach, CHS/CHSI and CHSPSC, LLC (hereafter “Defendants”) owned, leased or operated 206 affiliated hospitals in 29 states and these affiliates offered a broad range of health care services including inpatient and surgical services, outpatient treatment, and skilled nursing care.

### **DISCLOSURE OF BREACH AND RESPONSE**

12. In August 2014, Defendants publicly disclosed that in the preceding month CHSPSC had confirmed that its computer network had been accessed by intruders, first in April and again in June of 2014.

13. Defendants further disclosed that they believed the intruder had used malware to gain access to the company’s security systems and had successfully copied and transferred data, including the personal information of approximately 4.5 million patients that was on CHSPSC’s systems. After additional investigation, Defendants disclosed that the total number of patients whose personal information was accessed was approximately 6.1 million. The data taken related to patients of some of Defendants’ affiliated physician practices and clinics and included patients’ names, addresses, birthdates, social security numbers, and in some cases telephone numbers as well as the names of employers or guarantors. However, to the best of Defendants’ knowledge, no credit card information or medical or clinical information was taken.

14. Defendants also provided notice of the breach to government regulators and mailed notification letters to all affected patients informing them about the data breach. In these

letters Defendants offered affected patients the opportunity to enroll in free identity theft protection and credit monitoring services. Defendants also established a toll-free number and web site where affected patients could obtain additional information including how to access these services.

### **STATEMENT OF FACTS**

15. In the regular course of business, Defendants collect and maintain the personal information of individuals including individual names, addresses, dates of birth, and social security numbers.

16. Defendants also create, receive, use and maintain electronic Protected Health Information subject to the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.* (collectively, “HIPAA”). HIPAA and its Rules require the implementation of appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. *See*, 45 CFR Part 160 and Subparts A and C of Part 164.

17. Through its various policies, including a Privacy Policy and website Terms of Use, Defendants disclosed to consumers that they collected personal information, and generally explained what information was collected and the purpose for which it was collected and used, and the circumstances in which such information might be disclosed. Defendants also provided patients with the Notice of Privacy Protections as required by the HIPAA Privacy Rule.

18. In their disclosures to consumers, Defendants represented that they protected personal information, specifically that they treated the “...technical side of security seriously

[and] stored personal information ... on a secure server in a way that maximizes security and confidentiality,” and employed security measures to protect information from unauthorized disclosure through various means such as encryption.

19. Defendants engage in trade and commerce and do business in and throughout Illinois.

### **APPLICABLE LAW**

20. Section 2 of the Consumer Fraud Act provides:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the “Uniform Deceptive Trade Practices Act”, approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

21. Section 5 of the Personal Information Protection Act provides in part:

“Data collector” may include, but is not limited to, ...publicly held corporations, financial institutions, ... that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.” “Breach of the security of the system data” or “breach” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. ... “Personal information” means either of the following: (1) an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted by the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver’s license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account. ...

22. Section 45 of the Personal Information Protection Act, which became effective on January 1, 2017, provides in part:

(a) A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall

implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. ... (c) If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

(d) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.

### **VIOLATIONS**

#### **COUNT I - CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT**

23. The State of Illinois re-alleges and incorporates by reference each and every preceding paragraph of this petition.

24. Defendants, while engaged in trade or commerce, committed an unfair act or practice declared unlawful under Section 2 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, when it:

- A. Failed to implement and maintain reasonable security practices to protect consumers' personal information it collects and maintains;
- B. Failed to store personal information in a way that maximized its security and confidentiality; and
- C. Permitted the disclosure of Protected Health Information in a manner inconsistent with the requirements of HIPAA and its rules.

### **REMEDIES**

25. Section 7 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/7, provides:

Whenever the Attorney General has reason to believe that any person is using, has used, or is about to use any method, act or practice declared by the Act to be unlawful, and that

proceedings would be in the public interest, he may bring an action in the name of the State against such person to restrain by preliminary or permanent injunction the use of such method, act or practice. The Court, in its discretion, may exercise all powers necessary, including but not limited to: injunction, revocation, forfeiture or suspension of any license, charter franchise, certificate or other evidence of authority of any person to do business in this State; appointment of a receiver; dissolution of domestic corporations or association suspension or termination of the right of foreign corporations or associations to do business in this State; and restitution.

**PRAYER FOR RELIEF – COUNT I**

**WHEREFORE**, the Plaintiff respectfully requests this Honorable Court to issue an Order.

A. Finding that Defendants have violated Section 2 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, by engaging in the unlawful acts and practices herein;

B. Ordering Defendants to pay up to \$50,000 per deceptive act or unfair practices and an additional amount of \$50,000 for each act or practice found to have been committed with intent to defraud, as provided in Section 7 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/7;

C. Requiring the Defendants to pay all costs for prosecution and investigation of this action, as provided by Section 10 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/10;

D. Permanently enjoining Defendants from engaging in the aforementioned act, practices, methods of competition or any other practice in violation of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and

E. Providing any such other and further relief as the Court deems just, proper, and equitable under the circumstances.

## **COUNT II – PERSONAL INFORMATION PROTECTION ACT**

26. The State of Illinois re-alleges and incorporates by reference each and every preceding paragraph of this petition.

27. Defendants are data collectors under the Personal Information Protection “Act, 815 ILCS 530/5.

28. Defendants have violated Section 45 of the Personal Information Protection Act, 815 ILCS 530/45, by failing to implement and maintain reasonable security measures to protect records that contain personal information concerning an Illinois resident from unauthorized access, acquisition, destruction, use, modification, or disclosure.

### **REMEDIES**

29. Section 20 of the Personal Information Protection Act, 815 ILCS 530/20 provides that “A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.”

30. Section 7 of the Consumer Fraud Act, 815 ILCS 505/7, provides:

(a) Whenever the Attorney General has reason to believe that any person is using, has used, or is about to use any method, act or practice declared by the Act to be unlawful, and that proceedings would be in the public interest, he may bring an action in the name of the State against such person to restrain by preliminary or permanent injunction the use of such method, act or practice. The Court, in its discretion, may exercise all powers necessary, including but not limited to: injunction, revocation, forfeiture or suspension of any license, charter franchise, certificate or other evidence of authority of any person to do business in this State; appointment of a receiver; dissolution of domestic corporations or association suspension or termination of the right of foreign corporations or associations to do business in this State; and restitution.

(b) In addition to the remedies provided herein, the Attorney General may request and this Court may impose a civil penalty in a sum not to exceed \$50,000 against any person found by the Court to have engaged in any method, act or practice declared unlawful under this Act. In the event the court finds the method, act or practice to have been entered into with intent to defraud, the court has authority to impose a civil penalty in a sum not to exceed \$50,000 per violation.

31. Section 10 of the Consumer Fraud Act, 815 ILCS 505/10, provides that “[i]n any

action brought under the provisions of this Act, the Attorney General is entitled to recover costs for the use of this State.”

**PRAYER FOR RELIEF – COUNT II**

**WHEREFORE**, the Plaintiff respectfully requests this Honorable Court to issue an Order:

A. Finding that Defendants have violated Section 45 of the Personal Information Protection Act, 815 ILCS 530/45, and 2 of the Consumer Fraud and Deceptive Business Practices Act, 825 ILCS 505/2, by engaging in the unlawful acts and practices herein;

B. Ordering Defendants to pay up to \$50,000 per deceptive act or unfair practice and an additional amount of \$50,000 for each act or practice found to have been committed with intent to defraud, as provided in Section 7 of the Consumer Fraud and Deceptive Practices Act, 815 ILCS 505/7;

C. Requiring the Defendants to pay all costs for the prosecution and investigation of this action, as provided by Section 10 of the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/10;

D. Permanently enjoining Defendants from engaging in the aforementioned acts, practices, methods of competition or any other practice in violation of the Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, and the Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; and

F. Providing any such other and further relief as the Court deems just, proper, and equitable under the circumstances.

Respectfully submitted,

THE PEOPLE OF THE STATE OF  
ILLINOIS, by KWAME RAOUL,  
ATTORNEY GENERAL OF ILLINOIS

/s/ Matthew W. Van Hise

Matthew W. Van Hise, CIPP/US  
Assistant Attorney General  
Chief, Privacy Unit  
Consumer Fraud Bureau  
500 South Second Street  
Springfield, IL 62702  
Telephone: (217) 782-4436

/s/ Elizabeth Blackston

Elizabeth Blackston  
Assistant Attorney General  
Chief, Consumer Fraud Bureau, Southern Region

Ronak Shah  
Carolyn Friedman  
Assistant Attorneys General  
Illinois Attorney General's Office

Dated: October 8, 2020