

## STATE OF CONNECTICUT

RETURN DATE:	11/07/23	)	SUPERIOR COURT
STATE OF CONNECTICUT,		)	JUDICIAL DISTRICT
		)	OF HARTFORD
Plaintiff,		)	AT HARTFORD
v.		)	
INMEDIATA HEALTH GROUP, LLC,		)	
AND INMEDIATA TECHNOLOGIES, LLC,		)	
Defendants.		)	OCTOBER 17, 2023

### **COMPLAINT**

Plaintiff, the State of Connecticut (the “State” or the “Plaintiff”), appearing through Attorney General William Tong, brings this action against Defendants Inmediata Health Group, LLC, and Inmediata Technologies, LLC (collectively, “Inmediata”), for violations of the Connecticut Unfair Trade Practices Act (“CUTPA”), General Statutes § 42-110b, *et seq.*, Connecticut’s Safeguards Law, General Statutes § 42-471, and Connecticut’s Data Breach Notification Law, General Statutes § 36a-701b, stemming from a data breach exposing the personal information of approximately 1.5 million individuals between May 16, 2016 and January 15, 2019. In support thereof, Plaintiff alleges the following:

### **THE PARTIES**

1. Plaintiff is the State of Connecticut, represented by William Tong, Connecticut Attorney General, pursuant to CUTPA at the request of Bryan Cafferelli, Commissioner of Consumer Protection, and more specifically General Statutes § 42-110m, and pursuant to the Attorney General's authority under General Statutes §§ 42-471 and 36a-701b.

2. Defendant Inmediata Health Group, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Avenue,

San Patricio, San Juan, PR 00920, and a branch known as Inmediata Health Group Corp., is located at 200 South Tryon Street, Suite 1700, Charlotte, NC 28202.

3. Defendant Inmediata Technologies, LLC is a limited liability corporation incorporated in the Commonwealth of Puerto Rico. Its principal office is located at 636 Ave San Patricio, San Juan, PR 00920.

### **JURISDICTION**

4. At all times relevant to this Complaint, Inmediata was engaged in “trade” and “commerce” affecting consumers in Connecticut, as those terms are defined in General Statutes § 42-110a(4), insofar as Inmediata provided health care clearinghouse services to health care providers in Connecticut. Inmediata was also in possession of the “personal information” of Connecticut residents, as defined in General Statutes §§ 36a-701b(a)(2) and 42-471(c).

5. Venue is proper in this Court pursuant to General Statutes § 51-345(a)(3).

### **BACKGROUND**

6. Inmediata acts as a health care clearinghouse, facilitating financial and clinical transactions between health care providers and insurers across the United States.

7. In the regular course of business, Inmediata collects and maintains the personal information of individuals, including names, addresses, dates of birth, and Social Security numbers.

8. Inmediata also receives, uses, and maintains electronic Protected Health Information (“ePHI”) subject to the requirements of 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”).

9. HIPAA and its rules require the implementation of appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. *See* 45 CFR Part 160 and Subparts A and C of Part 164.

### **STATEMENT OF FACTS**

10. On January 15, 2019, the U.S. Department of Health & Human Services' Office of Civil Rights ("OCR") alerted Inmediata that the personal information held and maintained by Inmediata was exposed online.

11. Inmediata's investigation revealed that a coding issue allowed two webpages to be indexed by Bing Bot (a search engine web crawler) from May 16, 2016 and continuing through January 15, 2019, exposing the personal information of approximately 1.5 million individuals.

12. Inmediata failed to prevent or discover Bing Bot crawling on the exposed webpages despite readily available methods of prevention through the use of robots.txt Search Engine Optimization ("SEO").

13. Robots.txt, also known as the robots exclusion standard or protocol, is a text file located in the root or main directory of a website, which serves as an instruction for SEO spiders on which parts of a website they can and cannot crawl. Robots.txt files can be customized to expressly disallow access to particular webpages.

14. Inmediata admits that robots.txt scripting was not implemented until *after* the data breach. Further, Inmediata did not have practices in place to detect Bing Bot crawling on sensitive webpages.

15. In addition, a HIPAA security risk assessment conducted by a third-party vendor from August 2017 to February 2019 flagged many "high risk" security deficiencies in Inmediata's systems relating to account management, access controls, end-of-life practices, antivirus and

firewall protection, encryption, segmentation, scanning, vendor management, intrusion detection and prevention, and logging and monitoring.

16. Among the security deficiencies identified were risks that Inmediata knew or should have known about, including among others, failures to implement policies and procedures. For example, while Inmediata's password policy set forth requirements for length and complexity, the assessment reflected these requirements were not actually implemented.

17. Despite these data security failures, Inmediata boasted on its website that it provides "[i]ndustry leading security with our data safely stored in the cloud" and that it is "[c]ompliant with HIPAA, CMS, and ONC requirements."

18. Inmediata also made promises to clients that it would take appropriate steps to protect personal information from unauthorized disclosure, which Inmediata failed to do.

19. Furthermore, although OCR notified Inmediata of the data breach on January 15, 2019, Inmediata did not begin mailing direct notice letters to impacted consumers until over three months later, on April 22, 2019.

20. Inmediata's response to the data breach was disorganized and resulted in misaddressed notifications being sent to impacted consumers. This resulted not only in further impermissible disclosures of PHI in some cases, but also a substantial likelihood that certain impacted consumers never received proper, direct notice of the breach.

21. Inmediata's notices also failed to provide sufficient details or context as to why Inmediata possessed consumers' data, which may have caused recipients to dismiss the notices as illegitimate.

## **CAUSES OF ACTION**

### **COUNT ONE**

#### **Violations of Data Breach Notification Law**

22. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

23. Inmediata did not begin mailing direct notice letters to affected Connecticut residents until April 22, 2019, ninety-seven (97) days after OCR alerted Inmediata to the data breach.

24. Inmediata also misaddressed certain notices sent to impacted consumers, which resulted in further notice delays and/or failures.

25. Inmediata therefore violated General Statutes § 36a-701b which requires that “notice shall be made without unreasonable delay but not later than sixty days after the discovery” of a data breach.

26. Further, Inmediata’s failure to comply with General Statutes § 36a-701b, constitutes an unfair trade practice in violation of CUTPA.

## **COUNT TWO**

### **Violations of CUTPA**

27. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

28. CUTPA at General Statutes § 42-110b(a) states: “[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.”

29. CUTPA at General Statutes § 42-110a(4) states that the terms “trade” and “commerce” shall mean: “the advertising, the sale or rent or lease, the offering for sale or rent or lease, or the distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity, or thing of value in this state.”

30. While engaged in trade or commerce in Connecticut, Inmediata violated CUTPA

by representing to health care providers that it protects the personal information of Connecticut residents, either implicitly by collecting such personal information or explicitly as set forth in Paragraphs 17-18.

31. Contrary to these representations, Inmediata allowed two webpages to be indexed by Bing Bot, which resulted in the exposure of Connecticut residents' personal information, among other data security failures.

32. Such representations were likely to mislead health care providers acting reasonably under the circumstances into believing that personal information was safeguarded from misuse by third parties and were material to their decisions about whether or not to entrust Inmediata with this personal information.

33. Inmediata, in the course of conducting its business, failed to implement and maintain reasonable security procedures and practices appropriate to protect the personal information of Connecticut residents, and thus did not protect that personal information from unauthorized access, use, destruction, modification, or disclosure.

34. By engaging in the aforementioned acts or practices, Inmediata violated the public policy of the State of Connecticut, including the public policy set forth in General Statutes § 42-471, which requires the protection of personal information from misuse, and the public policy set forth in the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1938, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services Regulations, 45 C.F.A. §§ 160, *et seq.*

35. Inmediata's acts or practices, as described herein, are oppressive, unethical, immoral, and unscrupulous.

36. Inmediata's acts or practices, as described herein, caused substantial injury to consumers.

37. Inmediata therefore engaged in unfair or deceptive acts and practices in violation of General Statutes § 42-110b(a).

### **COUNT THREE**

#### **Civil Penalties (Violations Of CUTPA)**

38. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

39. Inmediata engaged in the acts and practices alleged herein when it knew or should have known that its conduct was unfair or deceptive, in violation of General Statutes § 42-110b(a), and, therefore, is liable for civil penalties of up to \$5,000 per willful violation pursuant to General Statutes § 42-110o(b).

### **COUNT FOUR**

#### **Violations of Safeguards Law**

40. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

41. General Statutes § 42-471(a) provides that: "any person in possession of personal information of another person shall safeguard the data, computer files, and documents containing the information from misuse by third parties . . ."

42. Inmediata was in possession of Connecticut residents' "personal information" as that term is defined in General Statutes § 42-471(c).

43. Inmediata failed to implement and maintain reasonable procedures to protect and safeguard the personal information of Connecticut residents.

44. Inmediata therefore failed to safeguard personal information in violation of General

Statutes § 42-471.

**COUNT FIVE**

**Civil Penalties (Violations of Safeguards Law)**

45. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

46. Inmediata engaged in the acts or practices alleged herein in violation of General Statutes § 42-471(a) prior to July 1, 2023 and therefore is liable for civil penalties of up to \$500 per violation pursuant to General Statutes § 42-471(e).



### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests that this Court enter judgment against Defendants Inmediata Health Group, LLC, and Inmediata Technologies, LLC, and enter an Order:

1. Finding that Defendants violated General Statutes § 36a-701b by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendants from continuing to engage in such unlawful acts and practices;

2. Finding that Defendants violated General Statutes § 42-110b, *et seq.*, by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendants from continuing to engage in such unlawful acts and practices;

3. Finding that Defendants violated General Statutes § 42-471 by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendants from continuing to engage in such unlawful acts and practices;

4. Requiring Defendants to pay civil penalties pursuant to General Statutes § 42-110o(b);

5. Requiring Defendants to pay civil penalties pursuant to General Statutes § 42-471(e);

6. Requiring Defendants to pay all costs and fees for the prosecution and investigation of this action pursuant to General Statutes § 42-110m;


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

The State hereby states that the amount in controversy is more than Fifteen Thousand Dollars (\$15,000.00), exclusive of interests and costs.

Dated at Hartford, Connecticut this 17<sup>th</sup> day of October, 2023.

PLAINTIFF,  
STATE OF CONNECTICUT

WILLIAM TONG  
ATTORNEY GENERAL

By:   
\_\_\_\_\_  
John Neumon, Juris # 439448  
Laura Martella, Juris # 430264  
*Assistant Attorneys General*

Michele Lucan, Juris #429605  
*Deputy Associate Attorney General/  
Chief of the Privacy Section*

Office of the Attorney General  
Privacy & Data Security Department  
165 Capitol Avenue  
Hartford, CT 06106  
Telephone: (860) 808-5440