IN THE COURT OF COMMON PLEAS
FRANKLIN COUNTY, OHIO

STATE OF OHIO ex rel. ATTORNEY GENERAL DAVE YOST 30 E. Broad Street, 14th Floor Columbus, Ohio 43215 Plaintiff,	)	CASE NO. JUDGE
v.	)	
INMEDIATA HEALTH GROUP, LLC 636 Ave San Patricio San Juan, PR 00920	)	
INMEDIATA TECHNOLOGIES, LLC 636 Ave San Patricio San Juan, PR 00920 Defendants.	)	

COMPLAINT AND REQUEST FOR DECLARATRY JUDGMENT, INJUNCTIVE RELIEF, AND CIVIL PENALTIES

Plaintiff, the State of Ohio, by and through Ohio Attorney General Dave Yost, (the "State" or the "Plaintiff"), brings this action against Defendants Inmediata Health Group, LLC, and Inmediata Technologies, LLC (collectively, "Inmediata"), for violations of Ohio's Data Breach Notification Law, R.C. 1349.19 *et seq*. 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:

I. THE PARTIES

1. Plaintiff, State of Ohio, through Attorney General Dave Yost, having reasonable cause to believe that violations of Ohio's private disclosure of security breach of computerized personal information data law has occurred, brings this action in the public interest and on behalf of the State of Ohio under the authority vested in the Attorney General by R.C. 1349.192(A)(1).

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.

II. JURISDICTION AND VENUE

4. At all times relevant to this Complaint, Inmediata was a "business entity" as defined in R.C. 1349.19(A)(2) that suffered a "breach of the security of the system" as defined in R.C. 1349.19(A)(1)(a). The breach contained "personal information," as defined in R.C. 1349.19(A)(7)(a), related to individuals in Ohio.

5. Venue is proper in this Court pursuant to R.C. 1349.192(A)(1) and Ohio Civ. R. 3(C)(3).

III. 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.

IV. 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, including Ohio residents.

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. 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.

V. CAUSES OF ACTION

COUNT ONE

VIOLATIONS OF OHIO'S PRIVATE DISCLOSURE OF SECURITY BREACH OF COMPUTERIZED PERSONAL INFORMATION LAW (DATA BREACH NOTIFICATION ACT), R.C. 1349.19

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 Ohio 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.

25. Inmediata's conduct violated Ohio's Data Breach Notification Act, R.C. 1349.19 in that:

- Inmediata experienced a breach of security of the system during the time period of May 6, 2016 – January 1, 2019 when Inmediata failed to prevent or discover Bing Bot crawling on exposed webpages. As a result, individuals' personal information was disclosed that Inmediata could have reasonably believed would cause a material risk of identity theft or other fraud to Ohioans.
- Inmediata was required to disclose the data breach to affected Ohio residents after Inmediata discovered or was notified of the breach no later than 45 days following its discovery as required by R.C. 1349.19(B)(1) and (2).
- On information and belief, Inmediata's delay in notifying Ohio residents was not due to law enforcement determining that disclosure of notification would impede a criminal investigation per R.C. 1349.19(D).

VI. 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 to:

1. Declare that Defendants violated R.C. 1349.19(B)(1) and (2) 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. Require that Defendants refrain from future violations of Ohio's Data Breach Notification Act, R.C. 1349.19 *et seq*.

3. Require Defendants to pay civil penalties pursuant to R.C. 1349.192(A)-(C).

4. Require Defendants to pay all costs associated with this matter pursuant to R.C. 1349.192(B).

5. Grant any such further relief as the Court may deem appropriate.

Respectfully submitted,

DAVE YOST
Ohio Attorney General

/s/ Melissa Smith
Melissa Smith (0083551)
Michael Ziegler (0042206)
Assistant Attorneys General
Consumer Protection Section
30 E. Broad St., Floor 14
Columbus, OH 43215
614.466.6112
614.466.3980
Melissa.Smith@OhioAGO.gov
Michael.Ziegler@OhioAGO.gov

Counsel for Plaintiff, State of Ohio