

1 Douglas S. Swetnam (IN State Bar #15860-49)  
2 Section Chief – Data Privacy & ID Theft Unit  
3 Office of Attorney General Curtis Hill Jr.  
302 W. Washington St., 5th Floor  
Indianapolis, IN 46204  
4 Email: douglas.swetnam@atg.in.gov  
5 Telephone: (317) 232-6294

6 Michael A. Eades (IN State Bar #31015-49)  
7 Deputy Attorney General  
8 Office of Attorney General Curtis Hill, Jr.  
302 W. Washington St., 5th Floor  
Indianapolis, IN 46204  
9 Email: Michael.Eades@atg.in.gov  
10 Telephone: (317) 234-6681

11 Taylor C. Byrley (IN State Bar #35177-49)  
12 Deputy Attorney General  
13 Office of Attorney General Curtis Hill Jr.  
302 W. Washington St., 5th Floor  
Indianapolis, IN 46204  
14 Email: Taylor.Byrley@atg.in.gov  
15 Telephone: (317) 234-2235  
Attorneys for Plaintiff State of Indiana

16 John C. Gray (Pro Hac Vice)  
17 Assistant Attorney General  
18 Office of Attorney General Mark Brnovich  
2005 N. Central Ave.  
Phoenix, AZ 85004  
19 Email: John.Gray@azag.gov  
20 Telephone: (602) 542-7753  
Attorney for Plaintiff State of Arizona

21 Peggy Johnson (Pro Hac Vice)  
22 Assistant Attorney General  
23 Office of Attorney General Leslie Rutledge  
323 Center St., Suite 200  
24 Little Rock, AR 72201  
25 Email: peggy.johnson@arkansasag.gov  
26 Telephone: (501) 682-8062  
Attorney for Plaintiff State of Arkansas

1 Diane Oates (Pro Hac Vice)  
2 Assistant Attorney General  
3 Office of Attorney General Pam Bondi  
4 110 Southeast 6th Street  
5 Fort Lauderdale, FL 33301  
6 Email: Diane.Oates@myfloridalegal.com  
7 Telephone: (954) 712-4603  
8 Attorney for Plaintiff State of Florida

9 William Pearson (Pro Hac Vice)  
10 Assistant Attorney General  
11 Office of Attorney General Tom Miller  
12 1305 E. Walnut, 2nd Floor  
13 Des Moines, IA 50319  
14 Email: William.Pearson@ag.iowa.gov  
15 Telephone: (515) 281-3731  
16 Attorney for Plaintiff State of Iowa

17 Sarah Dietz (Pro Hac Vice)  
18 Assistant Attorney General  
19 Office of Attorney General Derek Schmidt  
20 120 S.W. 10th Ave., 2nd Floor  
21 Topeka, KS 66612  
22 Email: sarah.dietz@ag.ks.gov  
23 Telephone: (785) 368-6204  
24 Attorney for Plaintiff State of Kansas

25 Kevin R. Winstead (Pro Hac Vice)  
26 Assistant Attorney General  
27 Office of Attorney General Andy Beshear  
28 1024 Capital Center Drive  
Frankfort, KY 40601  
Email: Kevin.Winstead@ky.gov  
Telephone: (502) 696-5389  
Attorney for Plaintiff Commonwealth of Kentucky

Alberto A. De Puy (Pro Hac Vice)  
Assistant Attorney General  
Office of Attorney General Jeff Landry  
1885 N. Third St.  
Baton Rouge, LA 70802  
Email: DePuyA@ag.louisiana.gov  
Telephone: (225) 326-6471

1 L. Christopher Styron (Pro Hac Vice)  
2 Assistant Attorney General  
3 Office of Attorney General Jeff Landry  
4 1885 N. Third St.  
5 Baton Rouge, LA 70802  
6 Email: styronl@ag.louisiana.gov  
7 Telephone: (225) 326-6400  
8 Attorneys for Plaintiff State of Louisiana

9 Jason T. Pleggenkuhle (Pro Hac Vice)  
10 Assistant Attorney General  
11 Office of Attorney General Lori Swanson  
12 Bremer Tower, Suite 1200  
13 445 Minnesota St.  
14 St. Paul, MN 55101-2130  
15 Email: jason.pleggenkuhle@ag.state.mn.us  
16 Telephone: (651) 757-1147  
17 Attorney for Plaintiff State of Minnesota

18 Daniel J. Birdsall (Pro Hac Vice)  
19 Assistant Attorneys General  
20 Office of Attorney General Doug Peterson  
21 2115 State Capitol  
22 PO Box 98920  
23 Lincoln, NE 68509  
24 Email: dan.birdsall@nebraska.gov  
25 Telephone: (402) 471-1279  
26 Attorney for Plaintiff State of Nebraska

27 Kimberley A. D'Arruda (Pro Hac Vice)  
28 Special Deputy Attorney General  
North Carolina Department of Justice  
Office of Attorney General Joshua H. Stein  
P.O. Box 629  
Raleigh, NC 27602-0629  
Email: kdarruda@ncdoj.gov  
Telephone: (919) 716-6013  
Attorney for Plaintiff State of North Carolina

1 Lara Sutherlin (Pro Hac Vice)  
2 Wisconsin Department of Justice  
3 Office of Attorney General Brad Schimel  
4 17 W. Main St., P.O. Box 7857  
5 Madison, WI 53707-7857  
6 Email: sutherlinla@doj.state.wi.us  
7 Telephone: (608) 267-7163  
8 Attorney for Plaintiff State of Wisconsin  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 **IN THE UNITED STATES DISTRICT COURT**  
2 **FOR THE NORTHERN DISTRICT OF INDIANA**

3 The States of Arizona; Arkansas; Florida;  
4 Indiana; Iowa; Kansas; Kentucky; Louisiana;  
5 Minnesota; Nebraska; North Carolina; and  
6 Wisconsin,

7 Plaintiffs;

8 vs.

9 Medical Informatics Engineering, Inc. d/b/a  
10 Enterprise Health, LLC and K&L Holdings, and  
11 NoMoreClipboard, LLC,

12 Defendants.

Case No.:

**COMPLAINT**

13 **COMPLAINT**

14 Plaintiffs, the states of Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky,  
15 Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin (collectively “Plaintiff States”),  
16 for their complaint against Defendants Medical Informatics Engineering, Inc., (“MIE”) operating  
17 as Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, (“NMC” together  
18 with MIE “Defendants”), allege:

19 **SUMMARY OF THE CASE**

20  
21 1. Intermittently between May 7, 2015 and May 26, 2015, unauthorized persons  
22 (“hackers”) infiltrated and accessed the inadequately protected computer systems of Defendants.  
23 During this time, the hackers were able to access and exfiltrate the electronic Protected Health  
24 Information (“ePHI”), as defined by 45 C.F.R. § 160.103, of 3.9 million individuals, whose PHI  
25 was contained in an electronic medical record stored in Defendants’ computer systems. Such  
26 personal information obtained by the hackers included names, telephone numbers, mailing  
27  
28

1 addresses, usernames, hashed passwords, security questions and answers, spousal information  
2 (names and potentially dates of birth), email addresses, dates of birth, and Social Security  
3 Numbers. The health information obtained by the hackers included lab results, health insurance  
4 policy information, diagnosis, disability codes, doctors' names, medical conditions, and  
5 children's name and birth statistics.  
6

7         2.         In fostering a security framework that allowed such an incident to occur,  
8 Defendants failed to take adequate and reasonable measures to ensure their computer systems  
9 were protected, failed to take reasonably available steps to prevent the breaches, failed to  
10 disclose material facts regarding the inadequacy of their computer systems and security  
11 procedures to properly safeguard patients' personal health information, failed to honor their  
12 promises and representations that patients' personal health information would be protected, and  
13 failed to provide timely and adequate notice of the incident, which caused significant harm to  
14 consumers across the United States.  
15

16         3.         Defendants' actions resulted in the violation of the state consumer protection, data  
17 breach, personal information protection laws and federal HIPAA statutes, as more fully outlined  
18 below. Plaintiffs seek to enforce said laws by bringing this action.  
19

20         4.         This action is brought, in their representative and individual capacities as  
21 provided by state and federal law, by the attorneys general of Arizona, Arkansas, Florida,  
22 Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and  
23 Wisconsin (collectively the "Attorneys General"). The plaintiffs identified in the paragraph are  
24 also referred to collectively as the "Plaintiff States."  
25

26         5.         The Plaintiff States bring this action pursuant to consumer protection, business  
27 regulation, and/or data security oversight authority conferred on their attorneys general,  
28

1 secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens*  
2 *patriae* and/or common law authority. These state laws authorize the Plaintiff States to seek  
3 temporary, preliminary, and permanent injunctive relief, civil penalties, attorneys' fees,  
4 expenses, costs, and such other relief to which the Plaintiff States may be entitled.  
5

6 6. This action is also brought by the Attorneys General of the Plaintiff States  
7 pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the  
8 Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. §  
9 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et*  
10 *seq.*(collectively, "HIPAA"), which authorize attorneys general to initiate federal district court  
11 proceedings and seek to enjoin violations of, and enforce compliance with HIPAA, to obtain  
12 damages, restitution, and other compensation, and to obtain such further and other relief as the  
13 court may deem appropriate.  
14

### 15 **JURISDICTION AND VENUE**

16  
17 7. This Court has jurisdiction over the federal law claims pursuant to 42 U.S.C.  
18 § 1320d-5(d), and 28 U.S.C. §§ 1331 and 1337(a). This Court has supplemental jurisdiction over  
19 the subject matter of the state law claims pursuant to 28 U.S.C. § 1367.  
20

21 8. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c).

22 9. The Attorneys General provided prior written notice of this action to the Secretary  
23 of HHS, as required by 42 U.S.C. § 1320d-5(d)(4). The Attorneys General have also provided a  
24 copy of this complaint to the Secretary of HHS. *Id.*  
25

26 10. At all times relevant to this matter, Defendants were engaged in trade and  
27 commerce affecting consumers in the States insofar as Defendants provided electronic health  
28

1 records services to health care providers in the States. Defendants also maintained a website for  
2 patients and client health care providers in the States.

3  
4 **PLAINTIFFS**

5 11. The Attorneys General are charged with, among other things, enforcement of the  
6 Deceptive Trade Practices Acts, the Personal Information Protection Acts, and the Breach  
7 Notification Acts. The Attorneys General, pursuant to 42 U.S.C. § 1320d-5(d), may also enforce  
8 HIPAA.  
9

10 12. The Attorneys General are the chief legal officers for their respective states and  
11 commonwealths. The Plaintiff States bring this action pursuant to consumer protection, business  
12 regulation, and/or data security oversight authority conferred on their attorneys general,  
13 secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens*  
14 *patriae* and/or common law authority.  
15

16 13. Plaintiff Attorneys General institute this action for injunctive relief, statutory  
17 damages, attorney fees, and the costs of this action against Defendants for violations of the  
18 Health Insurance Portability and Accountability Act of 1996, as amended by the Health  
19 Information Technology for Economic and Clinical Health (“HITECH”) Act, 42 U.S.C. §  
20 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et*  
21 *seq.*(collectively, “HIPAA”), and supplemental state law claims under Plaintiffs’ respective  
22 Unfair, Deceptive, or Abusive Acts or Practices (“UDAP”) statutes, Disclosure of Data Breach  
23 Statutes (also referred to as “Breach Notification Acts”), and Personal Information Protection  
24 Statutes (also referred to as “PIPA”), specifically:  
25  
26  
27  
28



State	Deceptive Acts	Data Breach	PIPA
Arizona:	Ariz. Rev. Stat. § 44-1521 <i>et seq.</i>		
Arkansas:	Ark. Code § 4-88-101 <i>et seq.</i>	Ark. Code § 4-110-105	Ark. Code § 4-110-101 <i>et seq.</i>
Florida:	Chapter 501, Part II, Florida Statutes	Section 501.171, Florida Statutes	Section 501.171(9), Florida Statutes
Indiana:	Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G)		Ind. Code § 24-4.9-3-3.5(f)
Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2	
Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02	Kan. Stat. § 50-6139b
Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990		
Louisiana:	La. Rev. Stat. § 51:1401 <i>et seq.</i>	La. Rev. Stat. 51:3071 <i>et seq.</i>	
Minnesota:	Minn. Stat. §§ 325D.43 <i>et seq.</i> ; Minn. Stat. §§ 325F.68 <i>et seq.</i>	Minn. Stat. § 325E.61	
Nebraska:	Neb. Rev. Stat. §§ 59-1602; 59-1608, 59-1614, and 87-301	Neb. Rev. Stat. § 87-806	
North Carolina	N.C. Gen. Stat. § 75-1.1, <i>et seq.</i>	N.C. Gen. Stat. § 75-65	N.C. Gen. Stat. § 75-60, <i>et seq.</i>
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26	Wis. Stat. § 134.98	Wis. Stat. §§ 146.82 and 146.84(2)(b)

**DEFENDANTS**

14. Defendant MIE is a citizen of the State of Indiana. MIE is a corporation that is incorporated in Indiana and has its principal place of business in Indiana at 6302 Constitution Drive, Fort Wayne, IN 46804.

1           15. Defendant NMC is a citizen of the State of Indiana. NMC is a wholly-owned  
2 subsidiary of MIE, is organized in Indiana, and has its principal place of business in Indiana at  
3 6312 Constitution Drive, Fort Wayne, IN 46804.

4           16. Prior to January 6, 2016, MIE also operated under the name of Enterprise Health.  
5 Enterprise Health was a division of MIE. On January 6, 2016, MIE formed Enterprise Health,  
6 LLC, which shares founders, officers, employees, offices, and servers with MIE and NMC.  
7

8           17. K&L Holdings, LLC is affiliated with MIE and has the same founders, officers,  
9 and occupies the same offices as MIE, NMC, and Enterprise Health. K&L Holdings, LLC owns  
10 the property that serves as the headquarters for K&L Holdings, LLC, MIE, NMC, and Enterprise  
11 Health.  
12

### 13   **FACTUAL ALLEGATIONS**

14  
15           18. MIE is a third-party provider that licenses a web-based electronic health record  
16 application, known as WebChart, to healthcare providers. MIE, through its subsidiary NMC, also  
17 provides patient portal and personal health records services to healthcare providers that enable  
18 patients to access and manage their electronic health records. Through its WebChart application,  
19 MIE provides electronic health services to physicians and medical facilities nationwide.  
20

21           19. At all relevant times, MIE's customers consisted of healthcare providers who  
22 were Covered Entities within the meaning of HIPAA. 45 C.F.R. § 160.103.

23           20. At all relevant times, MIE and NMC were Business Associates within the  
24 meaning of HIPAA. 45 C.F.R. § 160.103.  
25

26           21. As Business Associates, Defendants are required to comply with the HIPAA  
27 federal standards that govern the security of ePHI, including Security Rules. *See* 45 C.F.R. §  
28 164.302.

1           22.     The Security Rule generally prohibits Covered Entities and Business Associates,  
2 such as Defendants, from unlawfully disclosing ePHI. The Security Rule requires Covered  
3 Entities and Business Associates to employ appropriate Administrative, Physical, and Technical  
4 Safeguards to maintain the security and integrity of ePHI. *See* 45 C.F.R. § 164.302.  
5

6           23.     At all relevant times, no written agreement existed between MIE and its  
7 subsidiary NMC to appropriately safeguard the information created, received, maintained, or  
8 transmitted by the entities.

9           24.     Between May 7, 2015 and May 26, 2015, hackers infiltrated and accessed the  
10 computer systems of Defendants.  
11

12           25.     The hackers stole the ePHI of 3.9 million individuals whose health information  
13 was contained in an electronic medical records database stored on Defendants' computer  
14 systems.  
15

16           26.     On June 10, 2015, MIE announced a "data security compromise that has affected  
17 the security of some personal and protected health information relating to certain clients and  
18 individuals who have used a Medical Informatics Engineering electronic health record." *Medical*  
19 *Informatics Engineering Updates Notice to Individuals of Data Security Compromise*, MIE (July  
20 23, 2015), <http://www.mieweb.com/notice>.  
21

22           27.     On June 20, 2015, NMC announced "a data security compromise that has affected  
23 the security of some personal and protected health information relating to individuals who have  
24 used a NoMoreClipboard personal health record or patient portal." *NoMoreClipboard Notice to*  
25 *Individuals of a Data Security Compromise*, NoMoreClipboard (July 23, 2015),  
26 <https://www.nomoreclipboard.com/notice>.  
27  
28

1           28. Defendants admitted that unauthorized access to their network began on May 7,  
2 2015, but they did not discover the suspicious activity until May 26, 2015.

3           29. After discovering the intrusion, Defendants “began an investigation to identify  
4 and remediate any identified security vulnerability,” hired “a team of third-party experts to  
5 investigate the attack and enhance data security and protection,” and “reported this incident to  
6 law enforcement including the FBI Cyber Squad.” *MIE Notice*, <http://www.mieweb.com/notice>;  
7 *NoMoreClipboard Notice*, <https://www.nomoreclipboard.com/notice>;  
8

9           30. MIE admitted that the following information was accessed by the hackers: “an  
10 individual’s name, telephone number, mailing address, username, hashed password, security  
11 question and answer, spousal information (name and potentially date of birth), email address,  
12 date of birth, Social Security number, lab results, health insurance policy information, diagnosis,  
13 disability code, doctor’s name, medical conditions, and child’s name and birth statistics.” *MIE*  
14 *Notice*, <http://www.mieweb.com/notice>.  
15

16           31. NMC admitted that the following information was accessed by the hackers: “an  
17 individuals’ [sic] name, home address, Social Security number, username, hashed password,  
18 spousal information (name and potentially date of birth), security question and answer, email  
19 address, date of birth, health information, and health insurance policy information.”  
20 *NoMoreClipboard Notice*, <https://www.nomoreclipboard.com/notice>.  
21

22           32. Defendants began notifying affected individuals by mail on July 17, 2015. This  
23 was two months after the initial breach date of May 7, 2015, and over 50 days after the breach  
24 discovery date of May 26, 2015.  
25

26           33. Defendants did not conclude mailing notification letters until December 2015, six  
27 months after the breach discovery date of May 26, 2015.  
28

1           34. Defendants' security framework was deficient in several respects. Defendants  
2 failed to implement basic industry-accepted data security measures to protect individual's health  
3 information from unauthorized access. Specifically, Defendants set up a generic "tester" account  
4 which could be accessed by using a shared password called "tester" and a second account called  
5 "testing" with a shared password of "testing". In addition to being easily guessed, these generic  
6 accounts did not require a unique user identification and password in order to gain remote access.  
7 In a formal penetration test conducted by Digital Defense in January 2015, these accounts were  
8 identified as high risk, yet Defendants continued to employ the use of these accounts and, in fact,  
9 acknowledged establishing the generic accounts at the request of one of its' health care provider  
10 clients so that employees did not have to log-in with a unique user identification and password.

13           35. Defendants did not have appropriate security safeguards or controls in place to  
14 prevent exploitation of vulnerabilities within their system. The "tester" account did not have  
15 privileged access but did allow the attacker to submit a continuous string of queries, known as a  
16 SQL injection attack, throughout the database as an authorized user. The queries returned error  
17 messages that gave the intruder hints as to why the entry was incorrect, providing valuable  
18 insight into the database structure.

20           36. The vulnerability to an SQL injection attack was identified as a high risk during a  
21 penetration test performed by Digital Defense in 2014. Digital Defense recommended that  
22 Defendant "take appropriate measures to implement the use of parameterized queries, or ensure  
23 the sanitization of user input." Despite this recommendation, Defendants took no steps to remedy  
24 the vulnerability.  
25

26           37. The intruder used information gained from the SQL error messages to access the  
27 "checkout" account, which had administrative privileges. The "checkout" account was used to  
28

1 access and exfiltrate more than 1.1 million patient records from Defendants' databases. The SQL  
2 error exploit was also used to obtain a second privileged account called "dcarlson". The  
3 "dcarlson" account was used to access and exfiltrate more than 565,000 additional records that  
4 were stored in a database containing NMC patient records.  
5

6 38. On May 25, 2015, the attacker initiated a second method of attack by inserting  
7 malware called a "c99" cell on Defendants' system. This malware caused a massive number of  
8 records to be extracted from Defendants' databases. The huge document dump slowed down  
9 network performance to such an extent that it triggered a network alarm to the system  
10 administrator. The system administrator investigated the event and terminated the malware and  
11 data exfiltration on May 26, 2015.  
12

13 39. Defendant's post-breach response was inadequate and ineffective. While the c99  
14 attack was being investigated, the attacker continued to extract patient records on May 26 and  
15 May 28, using the privileged "checkout" credentials acquired through use of the SQL queries.  
16 On those two days, a total of 326,000 patient records were accessed.  
17

18 40. The breach was not successfully contained until May 29, when a security  
19 contractor hired by Defendant identified suspicious IP addresses which led the contractor to  
20 uncover the principal SQL attack method.  
21

22 41. Defendants failed to implement and maintain an active security monitoring and  
23 alert system to detect and alert on anomalous conditions such as data exfiltration, abnormal  
24 administrator activities, and remote system access by unfamiliar or foreign IP addresses. The  
25 significance of the absence of these security tools cannot be overstated, as two of the IP  
26 addresses used to access Defendants' databases originated from Germany. An active security  
27  
28

1 operations system should have identified remote system access by an unfamiliar IP address and  
2 alerted a system administrator to investigate.

3 42. Defendants' privacy policy, in effect at the time of the breach, stated: "Medical  
4 Informatics Engineering uses encryption and authentication tools (password and user  
5 identification) to protect your personal information...[O]ur employees are aware that certain  
6 information provided by our customers is confidential and is to be protected." Yet Defendants  
7 failed to encrypt the sensitive personal information and ePHI within MIE's computer systems, a  
8 protection that, had it been employed, would have rendered the data unusable.

9 43. Defendants' information security policies were deficient and poorly documented.  
10 For example, the incident response plan provided by Defendants was incomplete. There are  
11 several questions posed in the document that indicate it is still in a coordination or draft stage.  
12 Indeed, there is no documented evidence or checklist to indicate that Defendants followed their  
13 own incident response plan. Finally, there is no documentation that Defendants conducted  
14 HIPAA Security and Awareness training for 2013, 2014, or 2015, prior to the breach.

15 44. Defendants' actions caused harm to members of the Plaintiff States. Specifically,  
16 the victims are subject to emotional distress due to their personal information and ePHI being in  
17 the hands of unknown and untrusted individuals, in addition to the increased potential for harm  
18 that could result from instances of fraud.

## 19 **DEFENDANTS' LAW VIOLATIONS**

### 20 **Count I** 21 **Arizona: Violation of HIPAA Safeguards**

22 45. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44  
23 of this Complaint.  
24

1           46. Defendants' conduct constitutes violations of Administrative Safeguards,  
2 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

3           a. MIE failed to review and modify security measures needed to continue the  
4 provision of reasonable and appropriate protection of ePHI in accordance with the  
5 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
6 164.306(e).

7  
8           b. MIE failed to conduct an accurate and thorough assessment of the  
9 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
10 that it maintained in accordance with the implementation specifications of the Security  
11 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

12  
13           c. MIE failed to implement security measures sufficient to reduce risks and  
14 vulnerabilities to a reasonable and appropriate level in accordance with the  
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
16 164.308(a)(1)(ii)(B).

17  
18           d. MIE failed to implement procedures to regularly review records of  
19 information system activity, such as audit logs, access reports, and Security Incident  
20 tracking reports in accordance with the implementation specifications of the Security  
21 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

22  
23           e. MIE failed to implement policies and procedures that, based upon its  
24 access authorization policies, establish, document, review, and modify a user's right of  
25 access to a workstation, transaction, program, or process that includes ePHI in  
26 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).



1 f. MIE failed to implement policies and procedures to address Security  
2 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
3 harmful effects of security incidents known to MIE, or to document such Incidents and  
4 their outcomes in accordance with the implementation specifications of the Security Rule,  
5 45 C.F.R. § 164.308(a)(6)(ii).  
6

7 g. MIE failed to assign a unique name and/or number for identifying and  
8 tracking user identity in accordance with the implementation specifications of the  
9 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).  
10

11 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
12 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
13 164.312(a)(2)(iv).  
14

15 i. MIE failed to implement hardware, software, and/or procedural  
16 mechanisms that record and examine activity in information systems that contain or use  
17 ePHI, in violation of 45 C.F.R. § 164.312(b).  
18

19 j. MIE failed to implement procedures to verify that a person or entity  
20 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).  
21

22 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
23 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).  
24

25 47. Plaintiff, Arizona, is entitled to certain statutory damages pursuant to 42 U.S.C.  
26 1320d-5(d)(2).  
27

28  
**Count II**  
**Arizona: Violation of Ariz. Rev. Stat. § 44-1522**

48. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44  
of this Complaint.

1 49. The Defendants' conduct constitutes a violation of Ariz. Rev. Stat. § 44-1522.

2 50. The information security failings outlined in paragraphs 30 through 40 constitute  
3 unfair or deceptive acts in violation of Ariz. Rev. Stat. § 44-1522.

4 51. For example, MIE committed unfair or deceptive acts or practices by  
5 representing, in connection with the advertisement and sale of its services, that it maintained  
6 appropriate Administrative and Technical Safeguards to protect patients' ePHI and other  
7 appropriate measures to protect consumers' sensitive information, when such was not the case.  
8

9 52. Defendants' security failings were also likely to cause substantial injury to  
10 consumers, including identity theft, and such injury was not reasonably avoidable by the  
11 consumers themselves, particularly in light of Defendants' failure to notify consumers in the  
12 most expedient manner possible, nor would such injury be outweighed by any countervailing  
13 benefits to consumers or competition.  
14

15 53. Defendants' conduct was also willful, as, among other things, they knew or  
16 should have known that their unfair or deceptive acts or practices were unlawful.  
17

18 54. Plaintiff, Arizona, is entitled to injunctive relief, restitution to all affected persons,  
19 and disgorgement of Defendants' profits or revenues obtained by means of its unlawful conduct  
20 pursuant to Ariz. Rev. Stat. § 44-1528; civil penalties pursuant to Ariz. Rev. Stat. § 44-1531; and  
21 attorney fees and costs pursuant to Ariz. Rev. Stat. § 44-1534.  
22

23 **Count III**  
24 **Arkansas: Violation of HIPAA Safeguards**

25 55. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44  
26 of this Complaint.

27 56. Defendants' conduct constitutes violations of Administrative Safeguards,  
28 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

1           a.       MIE failed to review and modify security measures needed to continue the  
2 provision of reasonable and appropriate protection of ePHI in accordance with the  
3 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
4 164.306(e).

5  
6           b.       MIE failed to conduct an accurate and thorough assessment of the  
7 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
8 that it maintained in accordance with the implementation specifications of the Security  
9 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

10  
11           c.       MIE failed to implement security measures sufficient to reduce risks and  
12 vulnerabilities to a reasonable and appropriate level in accordance with the  
13 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
14 164.308(a)(1)(ii)(B).

15           d.       MIE failed to implement procedures to regularly review records of  
16 information system activity, such as audit logs, access reports, and Security Incident  
17 tracking reports in accordance with the implementation specifications of the Security  
18 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

19  
20           e.       MIE failed to implement policies and procedures that, based upon its  
21 access authorization policies, establish, document, review, and modify a user's right of  
22 access to a workstation, transaction, program, or process that includes ePHI in  
23 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

24  
25           f.       MIE failed to implement policies and procedures to address Security  
26 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
27 harmful effects of security incidents known to MIE, or to document such Incidents and  
28

1 their outcomes in accordance with the implementation specifications of the Security Rule,  
2 45 C.F.R. § 164.308(a)(6)(ii).

3 g. MIE failed to assign a unique name and/or number for identifying and  
4 tracking user identity in accordance with the implementation specifications of the  
5 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

7 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
8 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
9 164.312(a)(2)(iv).

10 i. MIE failed to implement hardware, software, and/or procedural  
11 mechanisms that record and examine activity in information systems that contain or use  
12 ePHI, in violation of 45 C.F.R. § 164.312(b).

14 j. MIE failed to implement procedures to verify that a person or entity  
15 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

17 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
18 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

19 57. Plaintiff, Arkansas, is entitled to certain statutory damages pursuant to 42 U.S.C.  
20 1320d-5(d)(2).

21  
22 **Count IV**  
**Arkansas: Deceptive Acts in Violation of Ark. § 4-88-101**

23 58. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44  
24 of this Complaint.

25 59. The Defendants' conduct constitutes a violation of Ark. Code § 4-88-108.

26 60. The information security failings outlined in paragraphs 30 through 40 constitute  
27 unfair or deceptive acts in violation of Ark. Code § 4-88-108.  
28

1 61. MIE committed an unfair or deceptive act by representing that it maintained  
2 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
3 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
4 violation of Ark. Code Ann. § 4-88-107(b) and Ark. Code Ann. § 4-88-108.  
5

6 62. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code § 4-88-  
7 113(a)(3), attorney's fees and costs pursuant to Ark. Code § 4-88-113(e), and injunctive relief  
8 pursuant to Ark. Code § 4-88-113(a)(1).  
9

10 **Count V**  
**Arkansas: Data Breach Violation of Ark. Code § 4-110-105**

11 63. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44  
12 of this Complaint.  
13

14 64. MIE failed to notify affected individuals or others of the Data Breach as required  
15 by Ark. Code § 4-110-105.

16 65. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
17 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
18 date range after the breach was discovered was between 52 days and six months.  
19

20 66. By waiting between 52 days and six months to notify affected individuals,  
21 Defendants violated Ark. Code § 4-110-105.

22 67. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-  
23 108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e),  
24 and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).  
25  
26  
27  
28

1 **Count VI**

2 **Arkansas: Failure to Implement Reasonable Procedures to Protect Personal Information in**  
3 **Violation of Ark. Code § 4-110-104(b)**

4 68. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44  
5 of this Complaint.

6 69. Defendants failed to implement and maintain reasonable procedures to protect and  
7 safeguard the unlawful disclosure of personal information in violation of Ark. Code § 4-110-  
8 104(b).

9 70. The information security failings outlined in paragraphs 30 through 40 constitute  
10 unreasonable safeguard procedures in violation of Ark. Code § 4-110-104(b).

11 71. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-  
12 108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e),  
13 and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).  
14

15 **Count VII**

16 **Florida: Violation of HIPAA Safeguards**

17 72. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44  
18 of this Complaint.

19 73. Defendants' conduct constitutes violations of Administrative Safeguards,  
20 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

21 a. MIE failed to review and modify security measures needed to continue the  
22 provision of reasonable and appropriate protection of ePHI in accordance with the  
23 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
24 164.306(e).  
25

26 b. MIE failed to conduct an accurate and thorough assessment of the  
27 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
28

1 that it maintained in accordance with the implementation specifications of the Security  
2 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

3 c. MIE failed to implement security measures sufficient to reduce risks and  
4 vulnerabilities to a reasonable and appropriate level in accordance with the  
5 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
6 164.308(a)(1)(ii)(B).

7  
8 d. MIE failed to implement procedures to regularly review records of  
9 information system activity, such as audit logs, access reports, and Security Incident  
10 tracking reports in accordance with the implementation specifications of the Security  
11 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

12  
13 e. MIE failed to implement policies and procedures that, based upon its  
14 access authorization policies, establish, document, review, and modify a user's right of  
15 access to a workstation, transaction, program, or process that includes ePHI in  
16 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

17  
18 f. MIE failed to implement policies and procedures to address Security  
19 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
20 harmful effects of security incidents known to MIE, or to document such Incidents and  
21 their outcomes in accordance with the implementation specifications of the Security Rule,  
22 45 C.F.R. § 164.308(a)(6)(ii).

23  
24 g. MIE failed to assign a unique name and/or number for identifying and  
25 tracking user identity in accordance with the implementation specifications of the  
26 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

1 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
2 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
3 164.312(a)(2)(iv).

4 i. MIE failed to implement hardware, software, and/or procedural  
5 mechanisms that record and examine activity in information systems that contain or use  
6 ePHI, in violation of 45 C.F.R. § 164.312(b).

7 j. MIE failed to implement procedures to verify that a person or entity  
8 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

9 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
10 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

11 74. Plaintiff, Florida, is entitled to certain statutory damages pursuant to 42 U.S.C.  
12 1320d-5(d)(2).

13  
14  
15 **Count VIII**

16 **Florida: Deceptive Acts in Violation of Section 501.204, Florida Statutes**

17 75. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44  
18 of this Complaint.

19 76. The Defendants' conduct constitutes a violation of Section 501.204, Florida  
20 Statutes.

21 77. The information security failings outlined in paragraphs 30 through 40 constitute  
22 unfair or deceptive acts in violation of Section 501.204, Florida Statutes.

23 78. MIE committed an unfair or deceptive act by representing that it maintained  
24 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
25 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
26 violation of Section 501.204, Florida Statutes.  
27  
28





1           87.     The information security failings outlined in paragraphs 30 through 40 constitute  
2 unreasonable safeguard procedures in violation of Section 501.171(4), Florida Statutes.

3           88.     Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.171(9)(b),  
4 Florida Statutes, attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and  
5 injunctive relief pursuant to Section 501.171(9), Florida Statutes.  
6

7   **Count XI**  
8   **Indiana: Violation of HIPAA Safeguards**

9           89.     Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44  
10 of this Complaint.

11           90.     Defendants' conduct constitutes violations of Administrative Safeguards,  
12 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

13                   a.     MIE failed to review and modify security measures needed to continue the  
14 provision of reasonable and appropriate protection of ePHI in accordance with the  
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
16 164.306(e).

17                   b.     MIE failed to conduct an accurate and thorough assessment of the  
18 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
19 that it maintained in accordance with the implementation specifications of the Security  
20 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

21                   c.     MIE failed to implement security measures sufficient to reduce risks and  
22 vulnerabilities to a reasonable and appropriate level in accordance with the  
23 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
24 164.308(a)(1)(ii)(B).

1 d. MIE failed to implement procedures to regularly review records of  
2 information system activity, such as audit logs, access reports, and Security Incident  
3 tracking reports in accordance with the implementation specifications of the Security  
4 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).  
5

6 e. MIE failed to implement policies and procedures that, based upon its  
7 access authorization policies, establish, document, review, and modify a user's right of  
8 access to a workstation, transaction, program, or process that includes ePHI in  
9 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).  
10

11 f. MIE failed to implement policies and procedures to address Security  
12 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
13 harmful effects of security incidents known to MIE, or to document such Incidents and  
14 their outcomes in accordance with the implementation specifications of the Security Rule,  
15 45 C.F.R. § 164.308(a)(6)(ii).  
16

17 g. MIE failed to assign a unique name and/or number for identifying and  
18 tracking user identity in accordance with the implementation specifications of the  
19 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).  
20

21 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
22 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
23 164.312(a)(2)(iv).  
24

25 i. MIE failed to implement hardware, software, and/or procedural  
26 mechanisms that record and examine activity in information systems that contain or use  
27 ePHI, in violation of 45 C.F.R. § 164.312(b).  
28

1 j. MIE failed to implement procedures to verify that a person or entity  
2 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

3 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
4 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

5  
6 91. Plaintiff, Indiana, is entitled to certain statutory damages pursuant to 42 U.S.C.  
7 1320d-5(d)(2).

8 **Count XII**

9 **Indiana: Deceptive Acts in Violation of Ind. Code § 24-5-0.5-3**

10 92. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44  
11 of this Complaint.

12 93. The Defendants' conduct constitutes a violation of Ind. Code § 24-5-0.5-3.

13 94. The information security failings outlined in paragraphs 30 through 40 constitute  
14 unfair or deceptive acts in violation of Ind. Code § 24-5-0.5-3.

15 95. MIE committed an unfair or deceptive act by representing that it maintained  
16 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
17 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
18 violation of Ind. Code § 24-5-0.5-3.

19 96. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-5-0.5-  
20 4(g), attorney fees and costs pursuant to Ind. Code § 24-5-0.5-4(c), and injunctive relief pursuant  
21 to Ind. Code § 24-5-0.5-4(c).

22 **Count XIII**

23 **Indiana: Failure to Implement Reasonable Procedures to Protect Personal Information in**  
24 **Violation of Ind. Code § 24-4.9-3-3.5**

25 97. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44  
26 of this Complaint.

1 98. Defendants failed to implement and maintain reasonable procedures to protect and  
2 safeguard the unlawful disclosure of personal information in violation of Ind. Code § 24-4.9-3-  
3 3.5(c).

4 99. The information security failings outlined in paragraphs 30 through 40 constitute  
5 unreasonable safeguard procedures in violation of Ind. Code § 24-5-0.5-3.5.

6 100. Defendants are not exempt from Ind. Code § 24-5-0.5-3.5, as the Defendants did  
7 not comply with a HIPAA compliancy plan. Ind. Code § 24-5-0.5-3.5(a)(6).

8 101. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-4.9-3-  
9 3.5(f)(2), attorney fees and costs pursuant to Ind. Code § 24-4.9-3-3.5(f)(3), and injunctive relief  
10 pursuant to Ind. Code § 24-4.9-3-3.5(f)(1).

11  
12  
13 **Count XIV**  
14 **Iowa: Violation of HIPAA Safeguards**

15 102. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of  
16 this Complaint.

17 103. Defendants' conduct constitutes violations of Administrative Safeguards,  
18 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

19 a. MIE failed to review and modify security measures needed to continue the  
20 provision of reasonable and appropriate protection of ePHI in accordance with the  
21 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
22 164.306(e).

23 b. MIE failed to conduct an accurate and thorough assessment of the  
24 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
25 that it maintained in accordance with the implementation specifications of the Security  
26 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

1 c. MIE failed to implement security measures sufficient to reduce risks and  
2 vulnerabilities to a reasonable and appropriate level in accordance with the  
3 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
4 164.308(a)(1)(ii)(B).  
5

6 d. MIE failed to implement procedures to regularly review records of  
7 information system activity, such as audit logs, access reports, and Security Incident  
8 tracking reports in accordance with the implementation specifications of the Security  
9 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).  
10

11 e. MIE failed to implement policies and procedures that, based upon its  
12 access authorization policies, establish, document, review, and modify a user's right of  
13 access to a workstation, transaction, program, or process that includes ePHI in  
14 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).  
15

16 f. MIE failed to implement policies and procedures to address Security  
17 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
18 harmful effects of security incidents known to MIE, or to document such Incidents and  
19 their outcomes in accordance with the implementation specifications of the Security Rule,  
20 45 C.F.R. § 164.308(a)(6)(ii).  
21

22 g. MIE failed to assign a unique name and/or number for identifying and  
23 tracking user identity in accordance with the implementation specifications of the  
24 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).  
25

26 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
27 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
28 164.312(a)(2)(iv).

1 i. MIE failed to implement hardware, software, and/or procedural  
2 mechanisms that record and examine activity in information systems that contain or use  
3 ePHI, in violation of 45 C.F.R. § 164.312(b).

4 j. MIE failed to implement procedures to verify that a person or entity  
5 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

6 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
7 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

8  
9 104. Plaintiff, Iowa, is entitled to certain statutory damages pursuant to 42 U.S.C.  
10 1320d-5(d)(2).

11  
12 **Count XV**  
13 **Iowa: Deceptive Acts in Violation of Iowa Code § 714.16**

14 105. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of  
15 this Complaint.

16 106. The Defendants' conduct constitutes a violation of Iowa Code § 714.16.

17 107. The information security failings outlined in paragraphs 30 through 40 constitute  
18 unfair or deceptive acts in violation of Iowa Code § 714.16.

19 108. MIE committed an unfair or deceptive act by representing that it maintained  
20 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
21 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
22 violation of Iowa Code § 714.16.  
23

24 109. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code § 714.16(8),  
25 attorney fees and costs pursuant to Iowa Code § 714.16(11), and injunctive relief pursuant to  
26 Iowa Code § 714.16(7).  
27

1 **Count XVI**  
2 **Iowa: Data Breach Violation of Iowa Code § 715C.2**

3 110. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of  
4 this Complaint.

5 111. MIE failed to notify affected individuals or others of the Data Breach as required  
6 by Iowa Code § 715C.2.

7  
8 112. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
9 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
10 date range after the breach was discovered was between 52 days and six months.

11 113. By waiting between 52 days and six months to notify affected individuals,  
12 Defendants violated Iowa Code § 715C.2.

13  
14 114. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code §§ 715C.2(9),  
15 714.16(7), attorney fees and costs pursuant to Iowa Code §§ 715C.2(9), 714.16(7), and  
16 injunctive relief pursuant to Iowa Code §§ 715C.2(9), 714.16(7).

17 **Count XVII**  
18 **Kansas: Violation of HIPAA Safeguards**

19 115. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44  
20 of this Complaint.

21 116. Defendants' conduct constitutes violations of Administrative Safeguards,  
22 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

23 a. MIE failed to review and modify security measures needed to continue the  
24 provision of reasonable and appropriate protection of ePHI in accordance with the  
25 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
26 164.306(e).  
27  
28



1           b.       MIE failed to conduct an accurate and thorough assessment of the  
2 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
3 that it maintained in accordance with the implementation specifications of the Security  
4 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

5  
6           c.       MIE failed to implement security measures sufficient to reduce risks and  
7 vulnerabilities to a reasonable and appropriate level in accordance with the  
8 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
9 164.308(a)(1)(ii)(B).

10  
11           d.       MIE failed to implement procedures to regularly review records of  
12 information system activity, such as audit logs, access reports, and Security Incident  
13 tracking reports in accordance with the implementation specifications of the Security  
14 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

15           e.       MIE failed to implement policies and procedures that, based upon its  
16 access authorization policies, establish, document, review, and modify a user's right of  
17 access to a workstation, transaction, program, or process that includes ePHI in  
18 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

19  
20           f.       MIE failed to implement policies and procedures to address Security  
21 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
22 harmful effects of security incidents known to MIE, or to document such Incidents and  
23 their outcomes in accordance with the implementation specifications of the Security Rule,  
24 45 C.F.R. § 164.308(a)(6)(ii).

1 g. MIE failed to assign a unique name and/or number for identifying and  
2 tracking user identity in accordance with the implementation specifications of the  
3 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

4 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
5 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
6 164.312(a)(2)(iv).

7 i. MIE failed to implement hardware, software, and/or procedural  
8 mechanisms that record and examine activity in information systems that contain or use  
9 ePHI, in violation of 45 C.F.R. § 164.312(b).

10 j. MIE failed to implement procedures to verify that a person or entity  
11 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

12 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
13 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

14 117. Plaintiff, Kansas, is entitled to certain statutory damages pursuant to 42 U.S.C.  
15 1320d-5(d)(2).

16  
17  
18  
19 **Count XVIII**  
20 **Kansas: Deceptive Acts in Violation of Kan. Stat. § 50-626**

21 118. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44  
22 of this Complaint.

23 119. The Defendants' conduct constitutes a violation of Kan. Stat. § 50-626.

24 120. The information security failings outlined in paragraphs 30 through 40 constitute  
25 unfair or deceptive acts in violation of Kan. Stat. § 50-626.

26 121. MIE committed an unfair or deceptive act by representing that it maintained  
27 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
28

1 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
2 violation of Kan. Stat. § 50-626.

3 122. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. § 50-636,  
4 attorney fees and costs pursuant to Kan. Stat. § 50-632(a)(4), and injunctive relief pursuant to  
5 Kan. Stat. § 50-632(a)(2).  
6

7 **Count XIX**  
8 **Kansas: Data Breach Violation of Kan. Stat. § 50-7a02**

9 123. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44  
10 of this Complaint.

11 124. MIE failed to notify affected individuals or others of the Data Breach as required  
12 by Kan. Stat. § 50-7a02.

13 125. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
14 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
15 date range after the breach was discovered was between 52 days and six months.  
16

17 126. By waiting between 52 days and six months to notify affected individuals,  
18 Defendants violated Kan. Stat. § 50-7a02.

19 127. Plaintiff, Kansas, is entitled to appropriate relief pursuant Kan. Stat. § 50-7a02(g).  
20

21 **Count XX**  
22 **Kansas: Failure to Implement Reasonable Procedures to Protect Personal Information in**  
23 **Violation of Kan. Stat. § 50-6139b(b)(1)**

24 128. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44  
25 of this Complaint.

26 129. Defendants failed to implement and maintain reasonable procedures to protect and  
27 safeguard the unlawful disclosure of personal information in violation of Kan. Stat. § 50-  
28 6139b(b)(1).

1 130. The information security failings outlined in paragraphs 30 through 40 constitute  
2 unreasonable safeguard procedures in violation of Kan. Stat. § 50-6139b(b)(1).

3 131. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. §§ 50-  
4 6139b(d, e), 50-636, attorney fees and costs pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636(c),  
5 and injunctive relief pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-632(a)(2).  
6

7 **Count XXI**  
8 **Kentucky: Violation of HIPAA Safeguards**

9 132. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through  
10 44 of this Complaint.

11 133. Defendants' conduct constitutes violations of Administrative Safeguards,  
12 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

13 a. MIE failed to review and modify security measures needed to continue the  
14 provision of reasonable and appropriate protection of ePHI in accordance with the  
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
16 164.306(e).  
17

18 b. MIE failed to conduct an accurate and thorough assessment of the  
19 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
20 that it maintained in accordance with the implementation specifications of the Security  
21 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).  
22

23 c. MIE failed to implement security measures sufficient to reduce risks and  
24 vulnerabilities to a reasonable and appropriate level in accordance with the  
25 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
26 164.308(a)(1)(ii)(B).  
27  
28

1           d.       MIE failed to implement procedures to regularly review records of  
2 information system activity, such as audit logs, access reports, and Security Incident  
3 tracking reports in accordance with the implementation specifications of the Security  
4 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

5  
6           e.       MIE failed to implement policies and procedures that, based upon its  
7 access authorization policies, establish, document, review, and modify a user's right of  
8 access to a workstation, transaction, program, or process that includes ePHI in  
9 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

10  
11           f.       MIE failed to implement policies and procedures to address Security  
12 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
13 harmful effects of security incidents known to MIE, or to document such Incidents and  
14 their outcomes in accordance with the implementation specifications of the Security Rule,  
15 45 C.F.R. § 164.308(a)(6)(ii).

16  
17           g.       MIE failed to assign a unique name and/or number for identifying and  
18 tracking user identity in accordance with the implementation specifications of the  
19 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

20  
21           h.       MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
22 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
23 164.312(a)(2)(iv).

24           i.       MIE failed to implement hardware, software, and/or procedural  
25 mechanisms that record and examine activity in information systems that contain or use  
26 ePHI, in violation of 45 C.F.R. § 164.312(b).

1 j. MIE failed to implement procedures to verify that a person or entity  
2 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

3 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
4 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

5  
6 134. Plaintiff, Kentucky, is entitled to certain statutory damages pursuant to 42 U.S.C.  
7 1320d-5(d)(2).

8 **Count XXII**

9 **Kentucky: Deceptive Acts in Violation of Ky. Rev. Stat. § 367.170**

10 135. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through  
11 44 of this Complaint.

12 136. The Defendants' conduct constitutes a violation of Ky. Rev. Stat. § 367.170.

13 137. The information security failings outlined in paragraphs 23 through 43 constitute  
14 unfair or deceptive acts in violation of Ky. Rev. Stat. § 367.170.

15 138. MIE committed an unfair or deceptive act by representing that it maintained  
16 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
17 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
18 violation of Ky. Rev. Stat. § 367.170.

19 139. Plaintiff, Kentucky, is entitled to civil penalties pursuant to Ky. Rev. Stat. §  
20 367.990(2), and injunctive relief pursuant to Ky. Rev. Stat. § 367.190.

21 **Count XXIII**

22 **Louisiana: Violation of HIPAA Safeguards**

23 140. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through  
24 44 of this Complaint.

1 141. Defendants' conduct constitutes violations of Administrative Safeguards,  
2 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

3 a. MIE failed to review and modify security measures needed to continue the  
4 provision of reasonable and appropriate protection of ePHI in accordance with the  
5 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
6 164.306(e).

7  
8 b. MIE failed to conduct an accurate and thorough assessment of the  
9 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
10 that it maintained in accordance with the implementation specifications of the Security  
11 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

12  
13 c. MIE failed to implement security measures sufficient to reduce risks and  
14 vulnerabilities to a reasonable and appropriate level in accordance with the  
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
16 164.308(a)(1)(ii)(B).

17  
18 d. MIE failed to implement procedures to regularly review records of  
19 information system activity, such as audit logs, access reports, and Security Incident  
20 tracking reports in accordance with the implementation specifications of the Security  
21 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

22  
23 e. MIE failed to implement policies and procedures that, based upon its  
24 access authorization policies, establish, document, review, and modify a user's right of  
25 access to a workstation, transaction, program, or process that includes ePHI in  
26 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

1 f. MIE failed to implement policies and procedures to address Security  
2 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
3 harmful effects of security incidents known to MIE, or to document such Incidents and  
4 their outcomes in accordance with the implementation specifications of the Security Rule,  
5 45 C.F.R. § 164.308(a)(6)(ii).  
6

7 g. MIE failed to assign a unique name and/or number for identifying and  
8 tracking user identity in accordance with the implementation specifications of the  
9 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).  
10

11 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
12 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
13 164.312(a)(2)(iv).  
14

15 i. MIE failed to implement hardware, software, and/or procedural  
16 mechanisms that record and examine activity in information systems that contain or use  
17 ePHI, in violation of 45 C.F.R. § 164.312(b).  
18

19 j. MIE failed to implement procedures to verify that a person or entity  
20 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).  
21

22 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
23 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).  
24

25 142. Plaintiff, Louisiana, is entitled to certain statutory damages pursuant to 42 U.S.C.  
26 1320d-5(d)(2).  
27

#### 28 **Count XXIV**

#### **Louisiana: Deceptive Acts in Violation of La. Rev. Stat. § 51:1405**

143. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through  
44 of this Complaint.



1 144. The Defendants' conduct constitutes a violation of La. Rev. Stat. § 51:1405.

2 145. The information security failings outlined in paragraphs 30 through 40 constitute  
3 unfair or deceptive acts in violation of La. Rev. Stat. § 51:1405.

4 146. MIE committed an unfair or deceptive act by representing that it maintained  
5 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
6 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
7 violation of La. Rev. Stat. § 51:1405.

8 147. Plaintiff, Louisiana, is entitled to civil penalties pursuant and injunctive relief  
9 pursuant to La. Rev. Stat. § 51:1407.

10  
11  
12 **Count XXV**  
13 **Louisiana: Data Breach Violation of La. Rev. Stat. § 51:3074**

14 148. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through  
15 44 of this Complaint.

16 149. MIE failed to notify affected individuals or others of the Data Breach as required  
17 by La. Rev. Stat. § 51:3074.

18 150. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
19 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
20 date range after the breach was discovered was between 52 days and six months.

21 151. By waiting between 52 days and six months to notify affected individuals,  
22 Defendants violated La. Rev. Stat. § 51:3074.

23 152. Plaintiff, Louisiana, is entitled to damages and civil penalties pursuant to La. Rev.  
24 Stat. 51:3075 and 16 La. Admin. Code Pt III, 701.  
25  
26  
27  
28

**Count XXVI**  
**Minnesota: Violation of HIPAA Safeguards**

153. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

154. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of

1 access to a workstation, transaction, program, or process that includes ePHI in  
2 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

3 f. MIE failed to implement policies and procedures to address Security  
4 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
5 harmful effects of security incidents known to MIE, or to document such Incidents and  
6 their outcomes in accordance with the implementation specifications of the Security Rule,  
7 45 C.F.R. § 164.308(a)(6)(ii).

8 g. MIE failed to assign a unique name and/or number for identifying and  
9 tracking user identity in accordance with the implementation specifications of the  
10 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

11 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
12 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
13 164.312(a)(2)(iv).

14 i. MIE failed to implement hardware, software, and/or procedural  
15 mechanisms that record and examine activity in information systems that contain or use  
16 ePHI, in violation of 45 C.F.R. § 164.312(b).

17 j. MIE failed to implement procedures to verify that a person or entity  
18 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

19 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
20 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

21 155. Plaintiff, Minnesota, is entitled to certain statutory damages pursuant to 42 U.S.C.  
22 1320d-5(d)(2).

1 **Count XXVII**

2 **Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325F.69**

3 156. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through  
4 44 of this Complaint.

5 157. Minnesota Statutes section 325F.69, subdivision 1 reads:

6 The act, use, or employment by any person of any fraud, false  
7 pretense, false promise, misrepresentation, misleading statement or  
8 deceptive practice, with the intent that others rely thereon in  
9 connection with the sale of any merchandise, whether or not any  
10 person has in fact been misled, deceived, or damaged thereby, is  
enjoinable as provided in section 325F.70

11 Minn. Stat. § 325F.69, subd. 1 (2017).

12 158. The term “merchandise” within the meaning of Minnesota Statutes section  
13 325F.69 includes services. *See* Minn. Stat. § 325F.68, subd. 2 (2017).

14 159. Defendants have repeatedly violated Minnesota Statutes section 325F.69,  
15 subdivision 1, by engaging in the deceptive and fraudulent practices described in this Complaint.  
16 For example, Defendants falsely represented to Minnesota persons that Defendants would protect  
17 and safeguard their protected health information and sensitive personal information—including,  
18 but not limited to, by using encryption tools and maintaining appropriate Administrative and  
19 Technical Safeguards to protect Minnesota persons’ ePHI, as well as other appropriate measures  
20 to protect Minnesota persons’ sensitive personal information—when such was not the case,  
21 resulting in the exposure of Minnesota persons’ protected health information and sensitive  
22 personal information as described in this Complaint.  
23  
24

25 160. As a result of the practices described in this Complaint, hackers accessed and  
26 exfiltrated the protected health information of more than 8,000 Minnesotans (including more  
27 than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The  
28

1 protected health information and sensitive personal information that was hacked includes an  
2 individual's name, telephone number, mailing address, username, hashed password, security  
3 question and answer, spousal information (including name and date of birth), email address, date  
4 of birth, Social Security number, lab results, health insurance policy information, diagnosis,  
5 disability code, doctor's name, medical conditions, and child's name and birth statistics. These  
6 Minnesota persons had their protected health information and personal information exposed in  
7 connection with their seeking treatment from healthcare providers, physician practices, hospitals,  
8 and/or other organizations which are or were located and/or operated within Minnesota.  
9

10  
11 161. Special circumstances exist that triggered a duty on the part of Defendants to  
12 disclose material facts related to vulnerabilities within Defendants' computer systems to  
13 Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants'  
14 computers systems, and that hackers had exposed these vulnerabilities, leading to the release of  
15 Minnesotans protected health information and personal information. Minnesotans did not have  
16 knowledge of these vulnerabilities or the release of this information at the time of their treatment.  
17 Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify  
18 Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did  
19 not say enough to prevent the representations it made to Minnesotans from being deceptive and  
20 misleading.  
21

22  
23 162. Defendants knew or had reason to know that Minnesotans would place their trust  
24 in Defendants and rely on Defendants to inform them of material facts relating to the  
25 vulnerabilities in Defendants' computers systems, and that hackers had exposed these  
26 vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing  
27 material facts, about these vulnerabilities.  
28



1 \*\*\*

2 (7) represents that goods or services are of a particular standard,  
3 quality, or grade, or that goods are of a particular style or model, if  
4 they are of another;

5 \*\*\* or

6 (13) engages in any other conduct which similarly creates a  
7 likelihood of confusion or of misunderstanding.

8 Minn. Stat. § 325D.44, subd. 1 (2017).

9 169. Defendants have repeatedly violated Minnesota Statutes section 325D.44,  
10 subdivision 1, by engaging in the deceptive and fraudulent conduct described in this Complaint,  
11 including by making false, deceptive, fraudulent, and/or misleading representations and material  
12 omissions to Minnesota persons regarding their products and services. These misrepresentations  
13 and material omissions include but are not limited to: (1) by making misrepresentations about  
14 protecting Minnesota persons ePHI and sensitive personal information, Defendants represented  
15 that their products and/or services had characteristics that they did not have in violation of Minn.  
16 Stat. § 325D.44, subd. 1(5), and were of a particular standard, quality, or grade, when they were  
17 of another in violation of Minn. Stat. § 325D.44, subd. 1(7); and (2) by falsely representing to  
18 Minnesota persons that Defendants would protect and safeguard their protected health  
19 information and sensitive personal information—including, but not limited to, by using  
20 encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect  
21 Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons'  
22 sensitive personal information—when such was not the case, resulting in the exposure of  
23 Minnesota persons' protected health information and sensitive personal information as described  
24 in this Complaint, Defendant engaged in conduct that creates a likelihood of confusing or of  
25 misunderstanding in violation of Minn. Stat. § 325D.44, subd. 1(13).  
26  
27  
28

1           170. As a result of the practices described in this Complaint, hackers accessed and  
2 exfiltrated the protected health information of more than 8,000 Minnesotans (including more  
3 than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The  
4 protected health information and sensitive personal information that was hacked includes an  
5 individual's name, telephone number, mailing address, username, hashed password, security  
6 question and answer, spousal information (including name and date of birth), email address, date  
7 of birth, Social Security number, lab results, health insurance policy information, diagnosis,  
8 disability code, doctor's name, medical conditions, and child's name and birth statistics. These  
9 Minnesota persons had their protected health information and personal information exposed as a  
10 result of their seeking treatment from healthcare providers, physician practices, hospitals, and/or  
11 other organizations which are or were located and/or operated within Minnesota.  
12

13  
14           171. Special circumstances exist that triggered a duty on the part of Defendants to  
15 disclose material facts related to vulnerabilities within Defendants' computer systems to  
16 Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants'  
17 computers systems, and that hackers had exposed these vulnerabilities, leading to the release of  
18 Minnesotans protected health information and personal information. Minnesota did not have  
19 knowledge of these vulnerabilities or the release of this information at the time of their treatment.  
20 Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify  
21 Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did  
22 not say enough to prevent the representations it made to Minnesotans from being deceptive and  
23 misleading.  
24

25  
26           172. Defendants knew or had reason to know that Minnesotans would place their trust  
27 in Defendants and rely on Defendants to inform them of material facts relating to the  
28



1 vulnerabilities in Defendants' computers systems, and that hackers had exposed these  
2 vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing  
3 material facts, about these vulnerabilities.  
4

5 173. Given the representations it made, its special knowledge, and the circumstances  
6 described in this Complaint, Defendants had a duty to disclose material facts to Minnesota  
7 persons in connection with the data breach described in this Complaint. By not doing so,  
8 Defendants failed to disclose material information in violation of Minnesota Statutes section  
9 325F.69, subdivision 1.  
10

11 174. Due to the deceptive and fraudulent conduct described in this Complaint,  
12 Minnesota persons made payments to Defendants for goods and services that they otherwise  
13 would not have purchased or in amounts that they should not have been required to pay.  
14

15 175. Defendants' conduct, practices, and actions described in this Complaint constitute  
16 multiple, separate violations of Minnesota Statutes section 325D.44.  
17

18 176. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31;  
19 attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat.  
20 § 8.31 and § 325D.45; restitution under the *parens patriae* doctrine, the general equitable powers  
21 of this Court, and § 8.31; and any such further relief as provided by law or equity, or as the Court  
22 deems appropriate and just.  
23

24 **Count XXIX**  
25 **Minnesota: Data Breach Violation of Minn. Stat. § 325E.61**

26 177. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through  
27 44 of this Complaint.  
28

178. MIE failed to notify affected individuals or others of the Data Breach as required  
by Minn. Stat. § 325E.61.

1           179. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
2 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
3 date range after the breach was discovered was between 52 days and six months.

4  
5           180. By waiting between 52 days and six months to notify affected individuals,  
6 Defendants violated Minn. Stat. § 325E.61.

7           181. Minnesota Statutes 325E.61, subdivision 1(a) provides in part that:

8                   Any person or business that conducts business in this state, and that  
9 owns or licenses data that includes personal information, shall  
10 disclose any breach of the security of the system following  
11 discovery or notification of the breach in the security of the data to  
12 any resident of this state whose unencrypted personal information  
was, or is reasonably believed to have been, acquired by an  
unauthorized person. The disclosure must be made in the most  
expedient time possible and without unreasonable delay.

13 Minn. Stat. § 325E.61, subd. 1(a) (2017).

14           182. At all relevant times, Defendants conducted business in Minnesota and owned or  
15 licensed data that included personal information.

16  
17           183. Defendants have violated Minnesota Statutes section 325E.61, subdivision 1(a) by  
18 failing to, without unreasonable delay, expediently notify Minnesota victims of the data breach  
19 described in this Complaint. Despite knowing that it exposed the personal information, including  
20 persons' names and Social Security numbers, of Minnesota persons, Defendants unreasonably  
21 delayed providing notice of this breach to Minnesota residents.

22  
23           184. Defendants' conduct, practices, and actions described in this Complaint constitute  
24 multiple, separate violations of Minnesota Statutes section 325E.61.

25           185. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31  
26 and § 325E.61, subd. 6; attorney fees and costs pursuant to Minn. Stat. § 8.31 and § 325E.61;  
27 subd. 6; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325E.61, subd. 6; restitution under  
28

1 the *parens patriae* doctrine, the general equitable powers of this Court, and Minn. Stat. § 8.31;  
2 and any such further relief as provided by law or equity, or as the Court deems appropriate and  
3 just.  
4

5 **Count XXX**  
6 **Nebraska: Violation of HIPAA Safeguards**

7 186. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through  
8 44 of this Complaint.

9 187. Defendants' conduct constitutes violations of Administrative Safeguards,  
10 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

11 a. MIE failed to review and modify security measures needed to continue the  
12 provision of reasonable and appropriate protection of ePHI in accordance with the  
13 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
14 164.306(e).  
15

16 b. MIE failed to conduct an accurate and thorough assessment of the  
17 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
18 that it maintained in accordance with the implementation specifications of the Security  
19 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).  
20

21 c. MIE failed to implement security measures sufficient to reduce risks and  
22 vulnerabilities to a reasonable and appropriate level in accordance with the  
23 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
24 164.308(a)(1)(ii)(B).  
25

26 d. MIE failed to implement procedures to regularly review records of  
27 information system activity, such as audit logs, access reports, and Security Incident  
28

1 tracking reports in accordance with the implementation specifications of the Security  
2 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

3 e. MIE failed to implement policies and procedures that, based upon its  
4 access authorization policies, establish, document, review, and modify a user's right of  
5 access to a workstation, transaction, program, or process that includes ePHI in  
6 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

7  
8 f. MIE failed to implement policies and procedures to address Security  
9 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
10 harmful effects of security incidents known to MIE, or to document such Incidents and  
11 their outcomes in accordance with the implementation specifications of the Security Rule,  
12 45 C.F.R. § 164.308(a)(6)(ii).

13  
14 g. MIE failed to assign a unique name and/or number for identifying and  
15 tracking user identity in accordance with the implementation specifications of the  
16 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

17  
18 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
19 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
20 164.312(a)(2)(iv).

21  
22 i. MIE failed to implement hardware, software, and/or procedural  
23 mechanisms that record and examine activity in information systems that contain or use  
24 ePHI, in violation of 45 C.F.R. § 164.312(b).

25  
26 j. MIE failed to implement procedures to verify that a person or entity  
27 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

1 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
2 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

3 188. Plaintiff, Nebraska, is entitled to certain statutory damages pursuant to 42 U.S.C.  
4 1320d-5(d)(2).  
5

6 **Count XXXI**  
7 **Nebraska: Deceptive Acts in Violation of Neb. Rev. Stat. § 59-1602**

8 189. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through  
9 44 of this Complaint.

10 190. The Defendants' conduct constitutes a violation of Neb. Rev. Stat. § 59-1602.

11 191. The information security failings outlined in paragraphs 30 through 40 constitute  
12 unfair or deceptive acts in violation of Neb. Rev. Stat. § 59-1602.

13 192. MIE committed an unfair or deceptive act by representing that it maintained  
14 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
15 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
16 violation of Neb. Rev. Stat. § 59-1602.  
17

18 193. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 59-  
19 1614, attorney fees and costs pursuant to Neb. Rev. Stat. § 59-1602(1), and injunctive relief  
20 pursuant to Neb. Rev. Stat. § 59-1608.  
21

22 **Count XXXII**  
23 **Nebraska: Data Breach Violation of Neb. Rev. Stat. § 87-803**

24 194. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through  
25 44 of this Complaint.

26 195. MIE failed to notify affected individuals or others of the Data Breach as required  
27 by Neb. Rev. Stat. § 87-803.  
28



1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
2 164.308(a)(1)(ii)(B).

3 d. MIE failed to implement procedures to regularly review records of  
4 information system activity, such as audit logs, access reports, and Security Incident  
5 tracking reports in accordance with the implementation specifications of the Security  
6 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

7 e. MIE failed to implement policies and procedures that, based upon its  
8 access authorization policies, establish, document, review, and modify a user's right of  
9 access to a workstation, transaction, program, or process that includes ePHI in  
10 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

11 f. MIE failed to implement policies and procedures to address Security  
12 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
13 harmful effects of security incidents known to MIE, or to document such Incidents and  
14 their outcomes in accordance with the implementation specifications of the Security Rule,  
15 45 C.F.R. § 164.308(a)(6)(ii).

16 g. MIE failed to assign a unique name and/or number for identifying and  
17 tracking user identity in accordance with the implementation specifications of the  
18 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

19 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
20 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
21 164.312(a)(2)(iv).

1 i. MIE failed to implement hardware, software, and/or procedural  
2 mechanisms that record and examine activity in information systems that contain or use  
3 ePHI, in violation of 45 C.F.R. § 164.312(b).

4 j. MIE failed to implement procedures to verify that a person or entity  
5 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

6 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
7 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

8  
9 201. Plaintiff, North Carolina, is entitled to certain statutory damages pursuant to 42  
10 U.S.C. 1320d-5(d)(2).

11  
12 **Count XXXIV**  
13 **North Carolina: Deceptive Acts in Violation of N.C. Gen. Stat. § 75-1.1**

14 202. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1  
15 through 44 of this Complaint.

16 203. The Defendants' conduct constitutes a violation of N.C. Gen. Stat. § 75-1.1.

17 204. The information security failings outlined in paragraphs 30 through 40 constitute  
18 unfair or deceptive acts in violation of N.C. Gen. Stat. § 75-1.1.

19 205. MIE committed an unfair or deceptive act by representing that it maintained  
20 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other  
21 appropriate measures to protect consumers' sensitive information, when such was not the case, in  
22 violation of N.C. Gen. Stat. § 75-1.1.

23  
24 206. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and  
25 injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq.*



1 **Count XXXV**

2 **North Carolina: Data Breach Violation of N.C. Gen. Stat. § 75-65**

3 207. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1  
4 through 44 of this Complaint.

5 208. MIE failed to notify affected individuals or others of the Data Breach as required  
6 by N.C. Gen. Stat. § 75-65.

7  
8 209. As alleged in paragraphs 28 and 29, Defendants began notifying affected  
9 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice  
10 date range after the breach was discovered was between 52 days and six months.

11 210. By waiting between 52 days and six months to notify affected individuals,  
12 Defendants violated N.C. Gen. Stat. § 75-65.

13  
14 211. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and  
15 injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq.*

16 **Count XXXVI**

17 **Wisconsin: Violation of HIPAA Safeguards**

18 212. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through  
19 44 of this Complaint.

20 213. Defendants' conduct constitutes violations of Administrative Safeguards,  
21 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

22 a. MIE failed to review and modify security measures needed to continue the  
23 provision of reasonable and appropriate protection of ePHI in accordance with the  
24 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
25 164.306(e).  
26  
27  
28

1           b.       MIE failed to conduct an accurate and thorough assessment of the  
2 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI  
3 that it maintained in accordance with the implementation specifications of the Security  
4 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

5  
6           c.       MIE failed to implement security measures sufficient to reduce risks and  
7 vulnerabilities to a reasonable and appropriate level in accordance with the  
8 implementation specifications of the Security Rule, in violation of 45 C.F.R. §  
9 164.308(a)(1)(ii)(B).

10  
11           d.       MIE failed to implement procedures to regularly review records of  
12 information system activity, such as audit logs, access reports, and Security Incident  
13 tracking reports in accordance with the implementation specifications of the Security  
14 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

15           e.       MIE failed to implement policies and procedures that, based upon its  
16 access authorization policies, establish, document, review, and modify a user's right of  
17 access to a workstation, transaction, program, or process that includes ePHI in  
18 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

19  
20           f.       MIE failed to implement policies and procedures to address Security  
21 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,  
22 harmful effects of security incidents known to MIE, or to document such Incidents and  
23 their outcomes in accordance with the implementation specifications of the Security Rule,  
24 45 C.F.R. § 164.308(a)(6)(ii).

1 g. MIE failed to assign a unique name and/or number for identifying and  
2 tracking user identity in accordance with the implementation specifications of the  
3 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

4 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in  
5 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §  
6 164.312(a)(2)(iv).

7 i. MIE failed to implement hardware, software, and/or procedural  
8 mechanisms that record and examine activity in information systems that contain or use  
9 ePHI, in violation of 45 C.F.R. § 164.312(b).

10 j. MIE failed to implement procedures to verify that a person or entity  
11 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

12 k. MIE failed to adhere to the Minimum Necessary Standard when using or  
13 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

14 214. Plaintiff, Wisconsin, is entitled to certain statutory damages pursuant to 42 U.S.C.  
15 1320d-5(d)(2).

16  
17  
18  
19 **Count XXXVII**

20 **Wisconsin: Fraudulent Representations in Violation of Wis. Stat. § 100.20**

21 215. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through  
22 44 of this Complaint.

23 216. The Defendants' conduct constitutes a violation of Wis. Stat. § 100.20.

24 217. MIE represented that it maintained appropriate Administrative and Technical  
25 Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers'  
26 sensitive information, when such was not the case, in violation of Wis. Stat. § 100.18.  
27

1           218. Plaintiff, Wisconsin, is entitled to civil penalties, attorney’s fees and costs, and  
2 injunctive relief pursuant to Wis. Stat. §§ 100.26 and 93.20.

3  
4   **Count XXXVIII**  
5           **Wisconsin: Negligent Disclosure of Patient Health Care Records in Violation of**  
6   **Wis. Stat. § 146.84(2)(b)**

7           219. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through  
8 44 of this Complaint.

9           220. The Defendants negligently disclosed confidential information in violation of  
10 Wis. Stat. § 146.82.

11           221. Plaintiff, Wisconsin, is entitled to civil penalties pursuant to Wis. Stat. §  
12 146.84(2)(b).

13  
14   **THIS COURT’S POWER TO GRANT RELIEF**

15           222. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow  
16 the Plaintiff States to enforce their state laws against Defendants in this Court and to grant such  
17 relief as provided under the following state laws including injunctive relief, civil penalties,  
18 attorneys’ fees, expenses, costs, and such other relief to which the Plaintiff States may be  
19 entitled:  
20

21

State	Deceptive Acts	Data Breach	PIPA
Arizona:	Ariz. Rev. Stat. §§ 44-1528, 44-1534, and 44-1531		
Arkansas:	Ark. Code Ann. § 4-88-113	Ark. Code Ann. § 4-110-108	Ark. Code Ann. § 4-110-108
Florida:	Sections 501.207, 501.2075, and 501.2105, Florida Statutes	Section 501.171(9), Florida Statutes	Section 501.171(9), Florida Statutes

22  
23  
24  
25  
26  
27  
28

1	Indiana:	Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G)		Ind. Code § 24-4.9-3-3.5(f)
2	Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2	
3	Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02	Kan. Stat. § 50-6139b
4	Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990		
5				
6	Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.	
7	Minnesota:	Minn. Stat. § 8.31	Minn. Stat. § 8.31	
8				
9	Nebraska:	Neb. Rev. Stat. §§ 59-1602; 59-1608, and 59-1614	Neb. Rev. Stat. § 87-806	
10				
11				
12	North Carolina	N.C. Gen. Stat. § 75-1.1, et seq.	N.C. Gen. Stat. § 75-65	N.C. Gen. Stat. § 75-60, et seq.
13				
14				
15	Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26		Wis. Stat. § 146.84(2)(b)
16				

**PRAYER FOR RELIEF**

WHEREFORE, the Plaintiff States respectfully request that the Court:

- A. Award Plaintiffs such injunctive relief as outlined in Exhibit A, to be filed concurrently herewith;
- B. Award Plaintiffs a financial judgment for restitution and civil penalties as permitted by statute, and;
- C. Award Plaintiffs such other relief the Court deems just and proper.

Respectfully Submitted,

Date: \_\_\_\_\_

Curtis T. Hill Jr.  
Attorney General of Indiana  
Atty. No. 13999-20

1  
2 By: /s/ Taylor C. Byrley  
3 Taylor C. Byrley, Deputy Attorney General  
4 Atty. No. 35177-49

5 By: /s/ Michael A. Eades  
6 Michael A. Eades, Deputy Attorney General  
7 Atty. No. 31015-49

8 By: /s/ Douglas S. Swetnam  
9 Douglas S. Swetnam, Section Chief  
10 Atty. No. 15860-49

11 Data Privacy and Identity Theft Unit  
12 Office of the Attorney General  
13 302 West Washington St., 5<sup>th</sup> Floor  
14 Indianapolis, IN 46204  
15 Tel: (317) 233-3300  
16 Taylor.Byrley@atg.in.gov  
17 Michael.Eades@atg.in.gov  
18 Douglas.Swetnam@atg.in.gov

19 Attorney General Mark Brnovich

20 By: /s/ John C. Gray  
21 John C. Gray (Pro Hac Vice)  
22 Assistant Attorney General  
23 Office of Attorney General Mark Brnovich  
24 2005 N. Central Ave.  
25 Phoenix, AZ 85004  
26 Email: John.Gray@azag.gov  
27 Telephone: (602) 542-7753  
28 Attorney for Plaintiff State of Arizona

1 Attorney General Leslie Rutledge

2 By: /s/ Peggy Johnson

3 Peggy Johnson (Pro Hac Vice)  
4 Assistant Attorney General  
5 Office of Attorney General Leslie Rutledge  
6 323 Center St., Suite 200  
7 Little Rock, AR 72201  
8 Email: peggy.johnson@arkansasag.gov  
9 Telephone: (501) 682-8062  
10 Attorney for Plaintiff State of Arkansas

11 Attorney General Pam Bondi

12 By: /s/ Diane Oates

13 Diane Oates (Pro Hac Vice)  
14 Assistant Attorney General  
15 Office of Attorney General Pam Bondi  
16 110 Southeast 6th Street  
17 Fort Lauderdale, FL 33301  
18 Email: Diane.Oates@myfloridalegal.com  
19 Telephone: (954) 712-4603  
20 Attorney for Plaintiff State of Florida

21 Attorney General Tom Miller

22 By: /s/ William Pearson

23 William Pearson (Pro Hac Vice)  
24 Assistant Attorney General  
25 Office of Attorney General Tom Miller  
26 1305 E. Walnut, 2nd Floor  
27 Des Moines, IA 50319  
28 Email: William.Pearson@ag.iowa.gov  
Telephone: (515) 281-3731  
Attorney for Plaintiff State of Iowa

1 Attorney General Derek Schmidt

2 By: /s/ Sarah Dietz

3 Sarah Dietz (Pro Hac Vice)  
4 Assistant Attorney General  
5 Office of Attorney General Derek Schmidt  
6 120 S.W. 10th Ave., 2nd Floor  
7 Topeka, KS 66612  
8 Email: sarah.dietz@ag.ks.gov  
9 Telephone: (785) 368-6204  
10 Attorney for Plaintiff State of Kansas

11 Attorney General Andy Beshear

12 By: /s/ Kevin R. Winstead

13 Kevin R. Winstead (Pro Hac Vice)  
14 Assistant Attorney General  
15 Office of Attorney General Andy Beshear  
16 1024 Capital Center Drive  
17 Frankfort, KY 40601  
18 Email: Kevin.Winstead@ky.gov  
19 Telephone: (502) 696-5389  
20 Attorney for Plaintiff Commonwealth of Kentucky

21 Attorney General Jeff Landry

22 By: /s/ Alberto A. De Puy

23 Alberto A. De Puy  
24 Assistant Attorney General  
25 Office of Attorney General Jeff Landry  
26 1885 N. Third St.  
27 Baton Rouge, LA 70802  
28 Email: DePuyA@ag.louisiana.gov  
Telephone: (225) 326-647

29 By: /s/ L. Christopher Styron

30 L. Christopher Styron (Pro Hac Vice)  
31 Assistant Attorney General  
32 Office of Attorney General Jeff Landry  
33 1885 N. Third St.  
34 Baton Rouge, LA 70802  
35 Email: styronl@ag.louisiana.gov  
36 Telephone: (225) 326-6400  
37 Attorneys for Plaintiff State of Louisiana



1 Attorney General Lori Swanson

2 By: /s/ Jason T. Pleggenkuhle  
3 Jason T. Pleggenkuhle (Pro Hac Vice)  
4 Assistant Attorney General  
5 Office of Attorney General Lori Swanson  
6 Bremer Tower, Suite 1200  
7 445 Minnesota St.  
8 St. Paul, MN 55101-2130  
9 Email: jason.pleggenkuhle@ag.state.mn.us  
10 Telephone: (651) 757-1147  
11 Attorney for Plaintiff State of Minnesota

12 Attorney General Doug Peterson

13 By: /s/ Daniel J. Birdsall  
14 Daniel J. Birdsall (Pro Hac Vice)  
15 Assistant Attorneys General  
16 Office of Attorney General Doug Peterson  
17 2115 State Capitol  
18 PO Box 98920  
19 Lincoln, NE 68509  
20 Email: dan.birdsall@nebraska.gov  
21 Telephone: (402) 471-1279  
22 Attorney for Plaintiff State of Nebraska

23 Attorney General Josh Stein

24 By: /s/ Kimberley A. D'arruda  
25 Kimberley A. D'Arruda (Pro Hac Vice)  
26 Special Deputy Attorney General  
27 North Carolina Department of Justice  
28 Office of Attorney General Joshua H. Stein  
P.O. Box 629  
Raleigh, NC 27602-0629  
Email: kdarruda@ncdoj.gov  
Telephone: (919) 716-6013  
Attorney for Plaintiff State of North Carolina

1 Attorney General Brad Schimel

2 By: /s/ Lara Sutherlin

3 Lara Sutherlin (Pro Hac Vice)

4 Wisconsin Department of Justice

5 Office of Attorney General Brad Schimel

6 17 W. Main St., P.O. Box 7857

7 Madison, WI 53707-7857

8 Email: sutherlinla@doj.state.wi.us

9 Telephone: (608) 267-7163

10 Attorney for Plaintiff State of Wisconsin

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28