UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

WESTEND DENTAL LLC, ARLINGTON WESTEND DENTAL LLC, SHERMAN WESTEND DENTAL LLC, FOUNTAIN SQUARE WESTEND DENTAL LLC, LAFAYETTE WESTEND DENTAL LLC, and AFFORDABLE WESTEND DENTAL LLC,

Defendants.

CASE NO. 1:24-cv-2255

COMPLAINT

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana and on behalf of the State of Indiana in its sovereign capacity (the "State"), by Deputy Attorneys General Douglas S. Swetnam and Jennifer M. Van Dame, brings this action for injunctive relief, statutory damages, civil penalties, attorney fees, costs, and other equitable relief against Westend Dental LLC, Arlington Westend Dental LLC, Sherman Westend Dental LLC, Fountain Square Westend Dental LLC, Lafayette Westend Dental LLC, and Affordable Westend Dental LLC (collectively, "Westend Dental") pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and

Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 (collectively, "HIPAA"), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq*. ("DSBA") and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq*. ("DCSA").

I. INTRODUCTION

1. This action stems from the State's investigation of Westend Dental, which was prompted by a consumer complaint from a Westend Dental patient regarding an unfulfilled request for dental records.

2. The Office of the Indiana Attorney General investigated Westend Dental's compliance with HIPAA, as well as the DSBA and DCSA.

3. During the State's investigation of the consumer complaint, the State discovered that Westend Dental experienced a ransomware attack on or around October 20, 2020, which exposed the personal information and protected health information ("PHI") of Indiana residents.

4. The exact number of Indiana residents affected by the breach is unknown because Westend Dental did not conduct a forensic investigation.

5. Although Westend Dental discovered the ransomware incident on or around October 20, 2020, and HIPAA requires notification within sixty (60) days after the discovery of a breach, 45 C.F.R. § 164.404(b), Westend Dental did not submit a data breach notification form to the State until October 28, 2022.

6. Even so, the data breach notification form that Westend Dental submitted on October 28, 2022, denied that a data breach occurred.

7. Westend Dental attempted to cover up the ransomware incident and

denied that a data breach occurred until a witness admitted during a sworn statement in January 2023 that a ransomware incident had occurred.

8. The State's investigation of the ransomware incident prompted the State to investigate Westend Dental's compliance with HIPAA generally. That investigation revealed, among other issues, that Westend Dental repeatedly disclosed PHI in public replies to online patient reviews and made public posts disclosing PHI and identifying individuals, including minor children, as patients of Westend Dental without patient authorization.

9. The State of Indiana has a long-held quasi-sovereign interest in protecting the health and welfare of its residents, which includes protecting residents from the loss of trust that results from a breach of doctor-patient confidentiality. It is well established that without trust in doctor-patient confidentiality, patients are more likely to withhold personal or sensitive information that may be important for health care providers to properly diagnose and treat patients and as a result, the quality of patient care declines.

II. PARTIES, JURISDICTION, AND VENUE

10. The Indiana Attorney General is authorized to bring this action to enforce HIPAA pursuant to 42 U.S.C. § 1320d-5(d).

11. The Indiana Attorney General is authorized to bring this action to enforce the DSBA pursuant to Ind. Code § 24-4.9-4-2, and the DCSA pursuant to Ind. Code § 24-5-0.5-4(c).

12. At all times relevant to this Complaint, Westend Dental LLC was an

Indiana limited liability company located in Indianapolis, Indiana, which was formed on November 20, 2015.

13. At all times relevant to this Complaint, Arlington Westend Dental LLC was an Indiana limited liability company located in Indianapolis, Indiana, which was formed on November 1, 2019.

14. At all times relevant to this Complaint, Sherman Westend Dental LLC was an Indiana limited liability company located in Indianapolis, Indiana, which was formed on January 24, 2017.

15. At all times relevant to this Complaint, Fountain Square Westend Dental LLC was an Indiana limited liability company located in Indianapolis, Indiana, which was formed on July 25, 2017.

16. At all times relevant to this Complaint, Lafayette Westend Dental LLC was an Indiana limited liability company located in Lafayette, Indiana, which was formed on November 28, 2017.

17. At all times relevant to this Complaint, Affordable Westend Dental LLC was an Indiana limited liability company located in Indianapolis, Indiana, which was formed on November 10, 2022.

18. Upon information and belief, each of the Westend Dental locations opened shortly after their respective limited liability company formed.

19. At all times relevant to this Complaint, Westend Dental provided dental products and services to Indiana patients and was a covered entity within the meaning of HIPAA. *See* 45 C.F.R. § 160.103.

20. At all times relevant to this Complaint, Westend Dental provided dental products and services to Indiana consumers and was engaged in trade and commerce affecting consumers in the State of Indiana. Westend Dental was also in possession of the personal information and PHI of Indiana residents.

21. This Court has jurisdiction pursuant to 42 U.S.C. § 1320d-5(d)(1) and 28 U.S.C. § 1331. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C § 1367.

22. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2).

23. The State has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. §1320d-5(d)(4).

III. HIPAA BACKGROUND

24. As a covered entity, Westend Dental was required to comply with the HIPAA standards that govern the security and privacy of PHI and notification to patients in the event of a breach. *See* 45 C.F.R. Part 164.

25. The HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) requires covered entities to ensure the confidentiality, integrity, and availability of all PHI that the covered entity creates, receives, maintains, or transmits and to protect against any reasonably anticipated threats to the security or integrity of such information. *See* 45 C.F.R. § 164.306. To this end, the HIPAA Security Rule requires covered entities to employ appropriate administrative, physical, and technical safeguards to maintain the security and integrity of PHI. *See* 45 C.F.R. §§ 164.308,

164.310, 164.312.

26. The HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D) requires covered entities to timely notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as a result of a breach. Notification must be provided "without unreasonable delay and **in no case later than 60 calendar days** after the discovery of a breach." 45 C.F.R. § 164.404(b) (emphasis added). "[A] breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity." 45 C.F.R. § 164.404(a)(2). Importantly, "Under this rule, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule." 78 Fed. Reg. 5648.

27. The HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) prohibits covered entities from using or disclosing PHI, except as permitted by HIPAA.

28. A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to PHI. *See* 45 C.F.R. § 160.103. HIPAA generally requires that covered entities enter into contracts with their business associates ("business associate agreements") to ensure that the business associates will appropriately safeguard

PHI. *See* 45 C.F.R. §§ 164.502(e) & 164.504(e).[1]

29. The statute of limitations for HIPAA violations is six (6) years. *See* 42 U.S.C. § 1320d-5(d)(8) & 42 U.S.C § 1320a–7a(c)(1).

IV. FACTUAL ALLEGATIONS

Background

30. Westend Dental offers dental products and services at various locations in central Indiana, including cleanings, checkups, fillings, root canal therapy, tooth extractions, dental crowns, dental bridges, braces, Invisalign, dental implants, dentures, teeth whitening, and porcelain veneers.[2]

31. Westend Dental is a series of dental practices that hold themselves out to the public as a single entity.[3]

32. Westend Dental accepts insurance for dental products and services.

33. Affordable Westend Dental LLC, Arlington Westend Dental LLC, Foutain Square Westend Dental LLC, Lafayette Westend Dental LLC, Sherman Westend Dental, LLC, and Westend Dental LLC are owned by Dr. Pooja Mandalia D.D.S. ("Dr. Mandalia").

34. Dr. Mandalia and Dr. Deept Rana D.D.S. ("Dr. Rana") are married.

35. A separate company called Westend Dental Management LLC is owned by Kunal Rana. Dr. Rana and Kunal Rana are brothers, but Kunal Rana is not a

[1] *Business Associate Contracts*, U.S. Dept. of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last visited Dec. 23, 2024).
[2] *Services*, Westend Dental, https://www.mywestenddental.com/services/ (last visited Dec. 23, 2024).
[3] *See* Westend Dental, https://www.mywestenddental.com/ (last visited Dec. 23, 2024) ("6 Convenient Locations").

dentist.

36. At all times relevant to this Complaint, every Westend Dental practice purportedly designated Dr. Rana as both its HIPAA Privacy Officer and HIPAA Security Officer, but this designation was never documented.

37. Before November 2023, Dr. Rana did not receive regular HIPAA training.

38. Despite not being an employee or contractor of Westend Dental, Kunal Rana has assisted in the management of operations at all Westend Dental locations.

39. Kunal Rana rents properties to Westend Dental, but aside from rent, he receives no other income from Westend Dental.

The Data Breach

40. On or around October 20, 2020, an unauthorized third-party (the "Intruder") deployed ransomware on a server containing PHI at the Arlington Westend Dental location (the "Data Breach").

41. On the date of the Data Breach, the Arlington Westend Dental location had at least 450 patients, but Westend Dental served at least 17,000 patients at all locations.

42. In order to deploy the ransomware, the Intruder gained access to at least the Arlington Westend Dental server, which contained the medical records of at least 450 patients – including:

a. Appointment details;

b. Biometric information;

c. Contact information;

d. Insurance information and coverage breakdowns;

e. Account information, such as payments made and due payments;

f. Treatment plans;

g. Dental charts and notes from previous appointments, if any;

h. Images, including scanned copies of New Patient forms, insurance verifications, and preauthorization letters; and

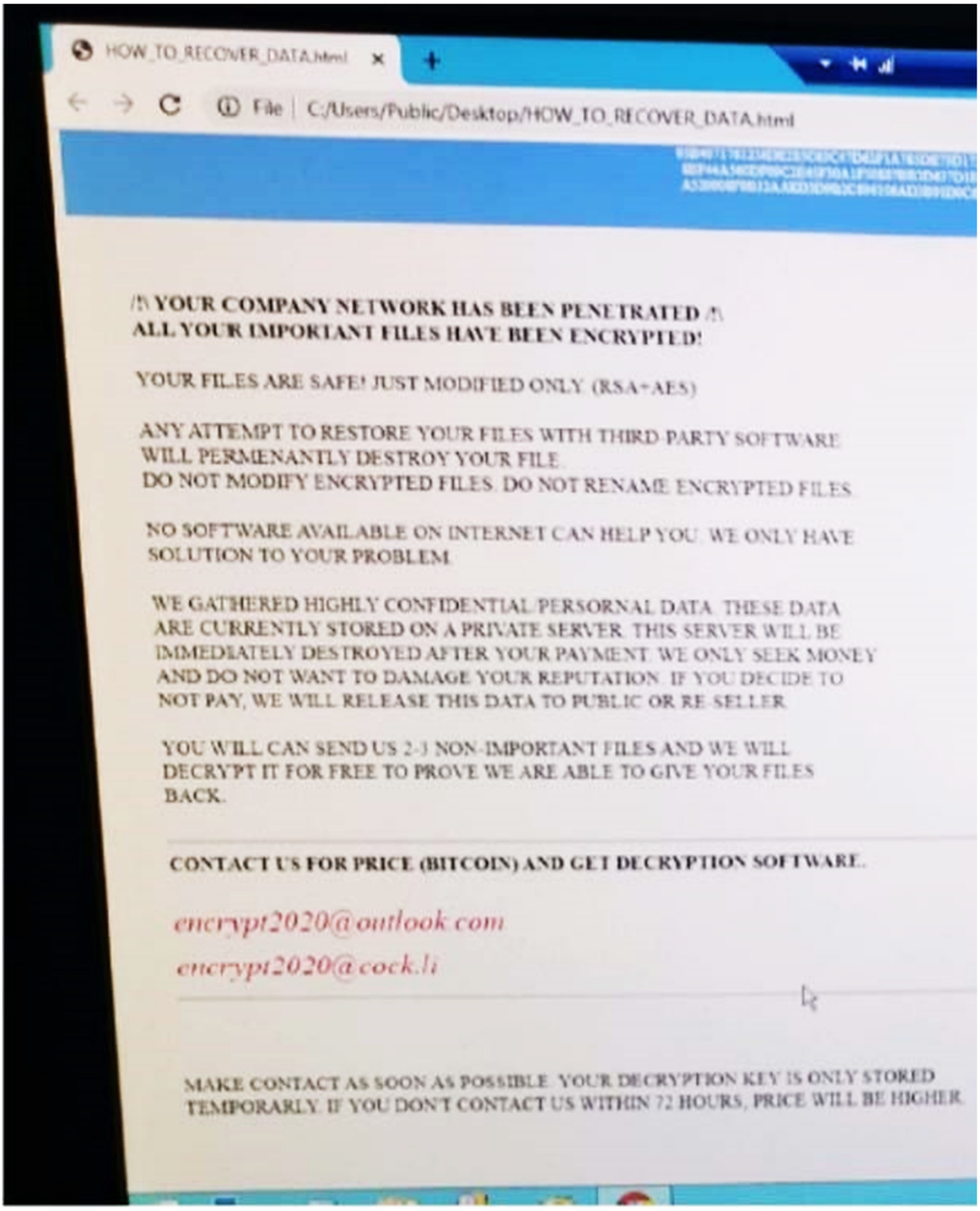
i. X-rays.

43. The ransomware deployed by the Intruder encrypted PHI stored on the Arlington Westend Dental server, rendering the encrypted PHI inaccessible.

44. The Intruder demanded payment in exchange for the encryption key to restore the PHI.

45. The following ransom note[4] was found on the Arlington Westend Dental server on October 20, 2020 ("Ransom Note"):

[4] The image has been cropped and enlarged for readability.



46. The Ransom Note directed Westend Dental to contact "encrypt2020@outlook.com", an email address associated with the ransomware group

MedusaLocker.[5]

47. According to the Cybersecurity & Infrastructure Security Agency ("CISA"), the national coordinator for critical infrastructure security and resilience, "MedusaLocker ransomware actors most often gain access to victim devices through vulnerable Remote Desktop Protocol (RDP) configurations."[6]

48. CISA also warns that MedusaLocker "frequently use[s] email phishing and spam email campaigns—directly attaching the ransomware to the email—as initial intrusion vectors."[7]

49. If the Intruder gained access to Westend Dental's system through a vulnerable Remote Desktop Protocol configuration, and Westend Dental did not address the vulnerable configuration, the Intruder would continue to have access to Westend Dental systems containing PHI.

50. For years after the Data Breach, Westend Dental did not address whether its Remote Desktop Protocol configuration was compromised.

51. Furthermore, at the time of the Data Breach, Westend Dental maintained lists of usernames and passwords for systems that contained PHI in plain text files.

52. At the time of the Data Breach, Westend Dental also used the same username and password combination for each of their servers that contained PHI.

---

[5] *Cybersecurity Advisory, #StopRansomware – MedusaLocker,* U.S. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a (last visited Dec. 23, 2024).
[6] *Id.*
[7] *Id.*

53. Likewise, at the time of the Data Breach, Westend Dental only used one (1) username and password combination for its SQL database that contained PHI.

54. Upon information and belief, at the time of the Data Breach, login credentials for the other systems that contained PHI were available on the compromised server at Arlington Westend Dental.

55. Upon information and belief, through access to the Arlington Westend Dental server, the Intruder gained access to Westend Dental's shared login credentials stored in plain text files, which gave the Intruder access to all Westend Dental systems and the PHI of all Westend Dental patients.

56. At the time of the Data Breach, Dr. Rana was Westend Dental's lead executive for IT-related matters. However, Dr. Rana was unable to recall during his sworn statement if there was a way to monitor network traffic at the time of the Data Breach.

57. At the time of the Data Breach, there was no logging or monitoring of access to Westend Dental databases containing PHI.

58. Westend Dental does not know if there were any suspicious logins to its databases storing PHI at the time of the Data Breach.

59. Upon information and belief, Westend Dental did not investigate whether there were any suspicious logins to databases storing PHI after the Data Breach.

60. Westend Dental had no systems in place to track who had access to or who had accessed PHI at the time of the Data Breach.

Data Breach Response and Failure to Provide Notification

61. At no time has Westend Dental completed a forensic investigation of the Data Breach.

62. Westend Dental has failed to investigate when the Intruder gained access to Westend Dental's systems and has failed to confirm the Intruder no longer has access to its systems.

63. In fact, Westend Dental has not even determined how the Intruder gained access to Westend Dental's systems.

64. After the Data Breach, Westend Dental was unable to recover patient files from any internal backups.

65. The backups provided to Westend Dental by a software vendor were incomplete and did not include all patient data affected by the Data Breach.

66. Westend Dental has never provided notification of the Data Breach to affected patients.

67. Westend Dental has never provided notification of the Data Breach to the media.

68. Westend Dental has never posted a notice of the Data Breach on its website or provided any other form of substitute notice.

Concealing the Data Breach

69. Westend Dental attempted to cover up the Data Breach.

70. Dr. Rana and his brother, Kunal Rana, have made false statements to the Office of the Indiana Attorney General ("OAG") regarding the Data Breach.

71. Westend Dental's attempt to cover up the Data Breach has delayed notification to Indiana residents, putting Indiana residents at a greater risk of harm.

72. Although Westend Dental was legally required to report the Data Breach directly to the OAG, the OAG discovered the Data Breach through its investigation of a consumer complaint made by a Westend Dental patient.

73. The OAG received a consumer complaint stating that the consumer had contacted Arlington Westend Dental on multiple occasions to receive copies of their x-rays, but Arlington Westend Dental stated it no longer had the x-rays because someone "hacked" their systems.

74. To investigate the consumer complaint, the OAG sent a request for information to Dr. Vijaya Palaparthi, a dentist at Arlington Westend Dental at the time of the Data Breach.

75. Dr. Palaparthi responded to the OAG's request in February 2022 by stating, in part: "We use several online applications that run on our server and facilitate patient care in our clinic. Unfortunately that also exposes our systems to some element of [sic]. Despite taking several security measures, our Server was infected with malware on the night of October 20, 2020."

76. On or around June 23, 2022, an OAG investigator contacted Westend Dental to inquire about the "malware" incident referenced in Dr. Palaparthi's response.

77. On or around October 28, 2022, two (2) years after the Data Breach, Westend Dental submitted a data breach notification form to the OAG indicating the

Data Breach affected fewer than 500 individuals and that "NO NOTICE" was provided to affected persons (the "Data Breach Notification Form").

78. The Data Breach Notification Form that Westend Dental submitted indicated the following types of information were involved in the Data Breach: (a) Name, (b) Address, (c) Driver's License/State ID Number, (d) Date of Birth, and (e) Protected Health Information.

79. However, Westend Dental's Data Breach Notification Form further stated, in relevant part:

> "THE INCIDENT WAS NOT OF DATA BREACH BUT OF LOSS OF DATA . . . THE PATIENT DATABASE GOT DELETED DURING ATTEMPTED MAINTENANCE OF THE SERVER TO IMPROVE ITS PERFORMANCE . . . THE PLAN WAS TO FORMAT THE HARD DRIVE PARTITION THAT DID NOT HAVE ANY PATIENT DATA . . . UNFORTUNATELY, THE ENTIRE HARD DRIVE, INCLUDING THE PARTITION THAT CONTAINED THE DATABASE WAS FORMATTED, AND DATA DELETED . . . WHILE PERFORMING RESTORATION OF DATA, SOME PATIENT'S DATA WAS NOT RECOVERED"

80. On November 4, 2022, an email sent from "kunal@daichidental.com" responded to the OAG's requests for additional information by stating, in relevant part:

> "This was not an intrusion, but an incident of data being lost when the on-site internal hard drive of the server got formatted by mistake. It is suspected the data was lost when we attempted to format a partition on the server hard drive that did not contain any database. The formatting process was not successful and the entire server hard drive data got lost in the incident. . . .
>
> The data server was not compromised by a ransomware attack and no ransom demands were received by the office. . . .
>
> This was not a ransomware attack. We did not receive any ransom

demand after the data was corrupted."

81. The November 4, 2022 email from "kunal@daichidental.com" lists Kunal Rana as the sender in the header.

82. The November 4, 2022 email to the OAG investigator also carbon copied "Deeptrana1981@gmail.com" and "Kunal135@gmail.com", Dr. Rana and Kunal Rana's personal email addresses, respectively.

83. On or around March 22, 2023, the OAG issued a civil investigative demand to Westend Dental.

84. On or around April 26, 2023, Westend Dental responded to the OAG's civil investigative demand.

85. In response to the civil investigative demand, Westend Dental stated, under penalty of perjury, that "No system was 'compromised.' Instead, data was lost on October 20th, 2020, when the on-site internal hard drive of the server was formatted by mistake', and "No patient had any data 'compromised.'"

86. Dr. Rana verified Westend Dental's written responses to the civil investigative demand.

87. Although the civil investigative demand requested "all communications regarding the incident" and "all communications relating to a malware attack," Westend Dental did not produce the photograph of the Ransom Note with its April 26, 2023 response. *See supra* Paragraph 45.

88. On or around October 30, 2023, Kunal Rana testified under oath pursuant to a civil investigative demand.

89. When asked, "Was there a ransomware attack on any of the Westend Dental entities on or around October 20th, 2020", Kunal Rana responded, "No, there wasn't."

90. When asked, "Was there a ransom note found on any Westend Dental entity's systems on or around October 20th, 2020?", Kunal Rana responded, "No."

91. However, shortly after October 20, 2020, Dr. Rana, Kunal Rana, and Heather Cramer, a Westend Dental Administrator, were in contact with Westend Dental's software vendor to assist in the recovery of their systems.

92. The OAG obtained copies of the customer service recordings between the software vendor and Westend Dental, which the OAG played for Kunal Rana at the end of his sworn statement on October 30, 2023.

93. During one customer service call on October 21, 2020, the software vendor told Kunal Rana and Heather Cramer that a server was infected with a "crypto virus," meaning the "database and a lot of the files on the system are not going to be accessible" because "they're all encrypted with . . . a nefarious person's virus".

94. In a subsequent customer service call on October 21, 2020, a different representative of the software vendor told Kunal Rana it was their understanding that Westend Dental "probably had some kind of crypto or ransomware attack yesterday, is that correct?" In response to this statement, Kunal Rana stated: "Yeah so we came to the office yesterday morning and we couldn't connect to the server and then when we got on the server we saw that all the files were encrypted. There was a message saying that we have to pay them to get the data back."

95. When asked about these customer service calls, Kunal Rana testified that it was the regular practice of Westend Dental to lie to employees and vendors in order to escalate IT issues more quickly and scare employees about using their work computers for personal use.

96. When specifically asked if he was lying to the software vendor when he said, "All the files were encrypted. There was a message saying that we have to pay them to get the data back", Kunal Rana responded, "I believe so."

97. However, after Kunal Rana's sworn statement, on or about December 6, 2023, Westend Dental produced the photograph of the Ransom Note to the OAG.

98. Thereafter, on January 10, 2024, Dr. Rana admitted during his sworn statement that Westend Dental experienced a ransomware attack.

99. This admission occurred over a year into the OAG's investigation, after multiple direct requests for information about the ransomware attack – all of which Westend Dental had answered with denials of a ransomware attack occurring.

100. Upon information and belief, the statements made under oath by Kunal Rana and by Westend Dental in interrogatory responses, denying the existence of a ransomware attack, were made to conceal the existence of a ransomware attack and resulting breach of Westend Dental patient information.

Social Media Protected Health Information Releases

101. Westend Dental has various online social media pages.

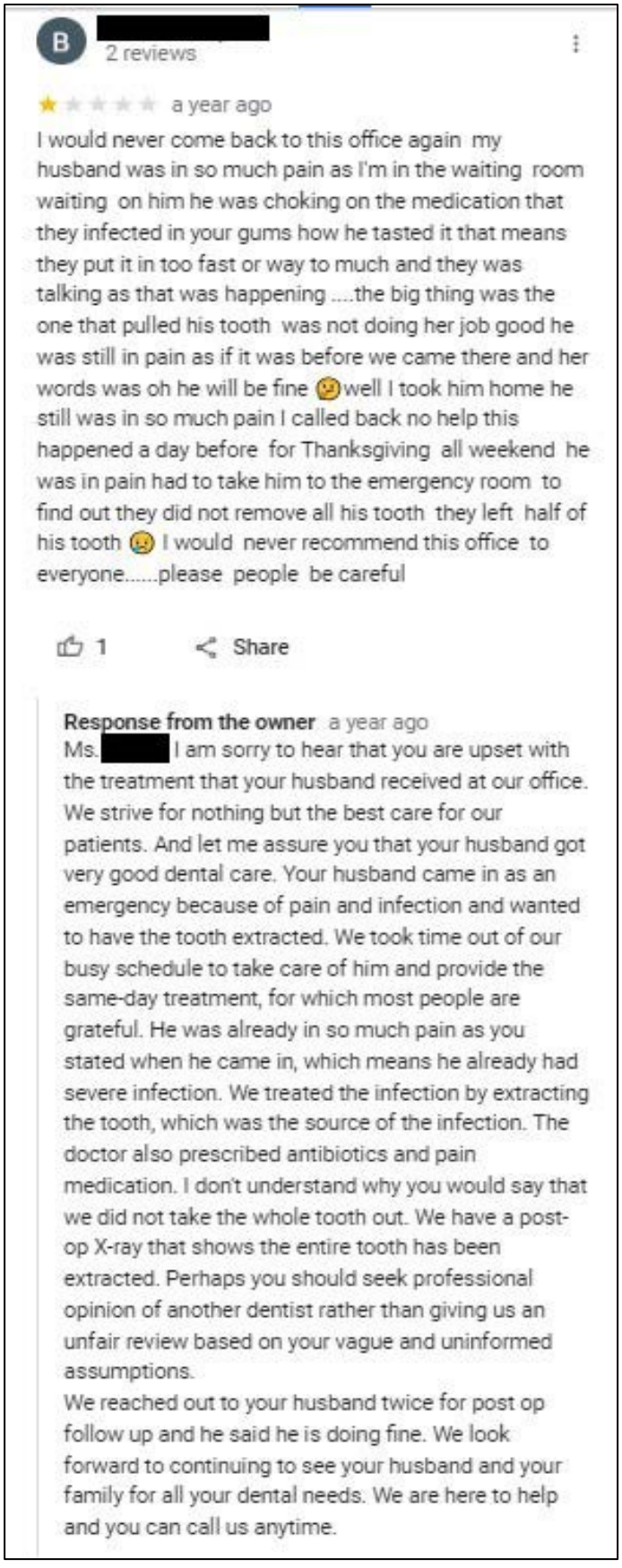
102. On multiple occasions, Westend Dental has posted public replies to online patient reviews.

103. Several of Westend Dental's public responses to online reviews have contained PHI.

104. Westend Dental never obtained the proper consent of any patient or minor patient's parent or guardian to use the patient's identity or PHI on social media.

105. For example, the following replies were made on Google Reviews, which appeared publicly on Westend Dental's Google business page as of October 31, 2023. These replies contain the PHI of Westend Dental patients, which was released without authorization.[8]

[8] Patient names have been redacted from all images. The exemplary images do not represent all replies the OAG located that improperly released PHI.



B [redacted]
2 reviews

★ a year ago

I would never come back to this office again my husband was in so much pain as I'm in the waiting room waiting on him he was choking on the medication that they infected in your gums how he tasted it that means they put it in too fast or way to much and they was talking as that was happening ....the big thing was the one that pulled his tooth was not doing her job good he was still in pain as if it was before we came there and her words was oh he will be fine 🤔well I took him home he still was in so much pain I called back no help this happened a day before for Thanksgiving all weekend he was in pain had to take him to the emergency room to find out they did not remove all his tooth they left half of his tooth 😢 I would never recommend this office to everyone.....please people be careful

1 Share

Response from the owner a year ago

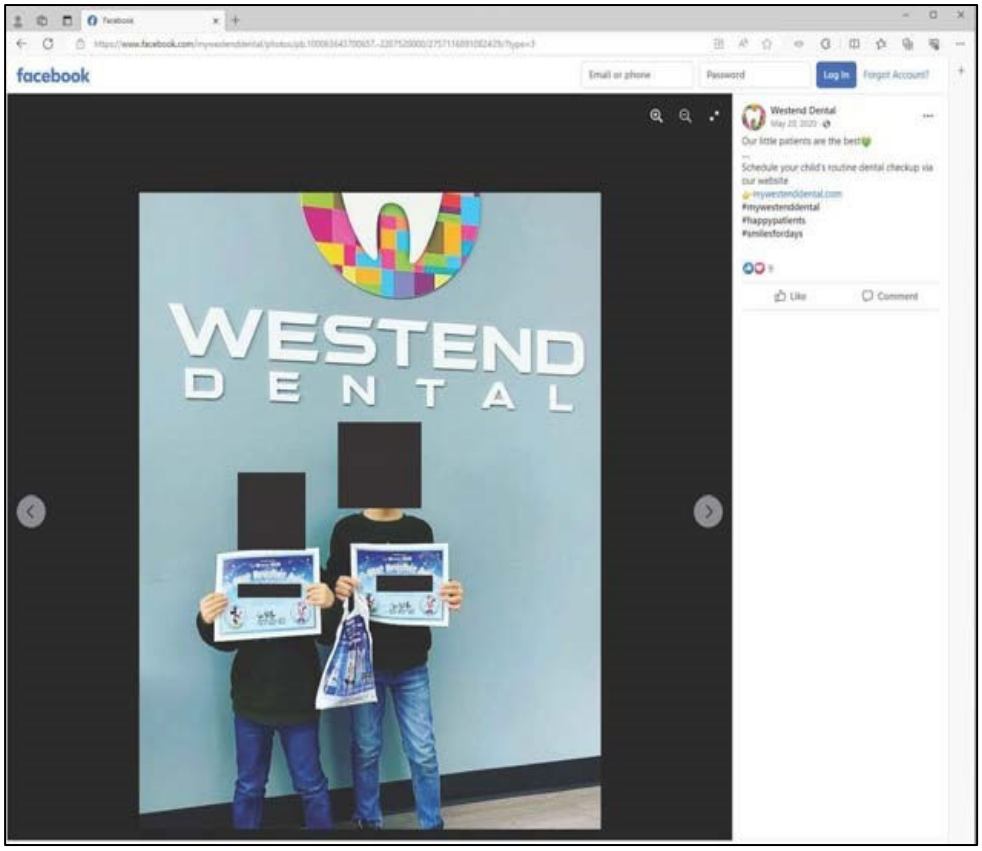
Ms. [redacted] I am sorry to hear that you are upset with the treatment that your husband received at our office. We strive for nothing but the best care for our patients. And let me assure you that your husband got very good dental care. Your husband came in as an emergency because of pain and infection and wanted to have the tooth extracted. We took time out of our busy schedule to take care of him and provide the same-day treatment, for which most people are grateful. He was already in so much pain as you stated when he came in, which means he already had severe infection. We treated the infection by extracting the tooth, which was the source of the infection. The doctor also prescribed antibiotics and pain medication. I don't understand why you would say that we did not take the whole tooth out. We have a post-op X-ray that shows the entire tooth has been extracted. Perhaps you should seek professional opinion of another dentist rather than giving us an unfair review based on your vague and uninformed assumptions.

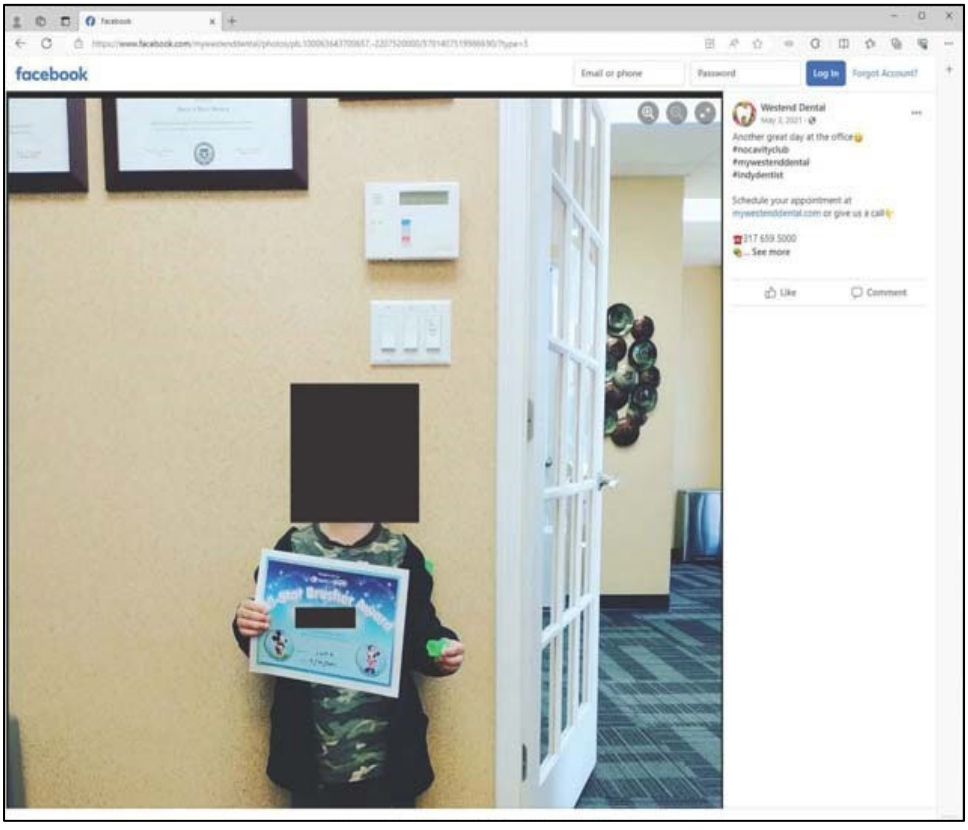
We reached out to your husband twice for post op follow up and he said he is doing fine. We look forward to continuing to see your husband and your family for all your dental needs. We are here to help and you can call us anytime.

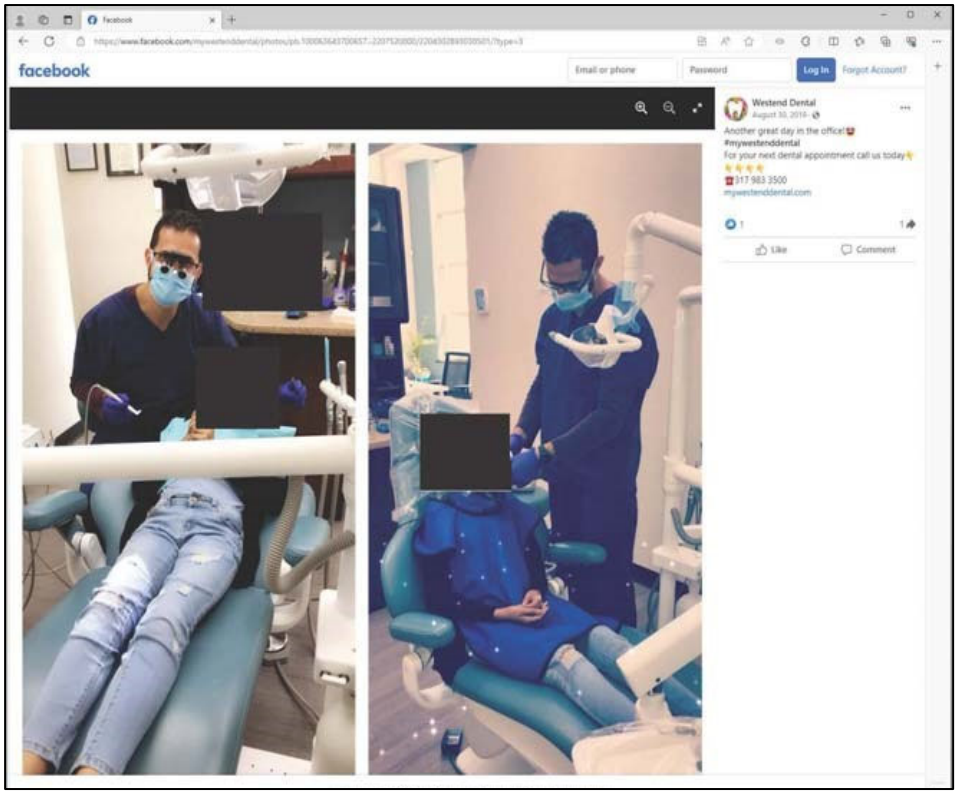
106. On multiple other occasions, Westend Dental made public posts identifying individuals, including minor children, as patients of Westend Dental.

107. For example, Westend Dental made the following public posts on Facebook. All of the following posts were public on Facebook as of November 6, 2023:[9]

[9] Patient faces, names, and x-rays have been redacted. The exemplary images do not represent all posts the OAG located that improperly released PHI.


facebook
Email or phone
Password
Log In
Forgot Account?
Westend Dental
Our little patients are the best!
Schedule your child's routine dental checkup via our website
#mywestenddental
#happypatients
#smilesfordays
Like
Comment
WESTEND
DENTAL


facebook
Email or phone
Password
Log In
Forgot Account?
Westend Dental
Another great day at the office
#nocavityclub
#mywestenddental
#indydentist
Schedule your appointment at mywestenddental.com or give us a call
217 659 5000
See more
Like
Comment



108. These Facebook posts contain the PHI of Westend Dental patients, including clearly visible x-rays, which were released without patient authorization.

Lack of HIPAA Policies and Procedures

109. Prior to November 2023, Westend Dental's HIPAA policies were stored in hardcopy at one location (the "Pre-2023 HIPAA Policies").

110. The Pre-2023 HIPAA Policies were never given to and were not readily available to any Westend Dental employees.

111. Upon information and belief, prior to November 2023, Westend Dental had not actually implemented any HIPAA policies.

112. Prior to November 2023, Westend Dental did not have HIPAA training for employees.

113. On or around November 20, 2023, after the OAG began investigating

the Data Breach, Westend Dental began using a third-party HIPAA compliance product that provides model policies, trainings, and a checklist for HIPAA compliance.

114. Notwithstanding Westend Dental's incorporation of a third-party HIPAA compliance product, Westend Dental continues to fail to comply with HIPAA.

115. For instance, HIPAA, specifically 45 C.F.R. § 164.520, requires covered entities to provide patients with a notice of privacy practices that contains the information specified in that regulation.

116. 45 C.F.R. § 164.520(c)(3)(i) further provides: "A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site."

117. However, Westend Dental does not post or make available on its website a notice of privacy practices that contains the information required by 45 C.F.R. § 164.520 (a "HIPAA Notice of Privacy Practices").

118. During Dr. Rana's sworn statement on January 10, 2024, Dr. Rana was questioned about a HIPAA Notice of Privacy Practices not being posted on Westend Dental's website.

119. At that time, Westend Dental had marked on the checklist provided by the third-party compliance product that Westend Dental complies with HIPAA's requirement to post a HIPAA Notice of Privacy Practices on its website.

120. However, Dr. Rana admitted in his January 10, 2024 sworn statement

that a HIPAA Notice of Privacy Practices was not posted on Westend Dental's website.

121. As of December 23, 2024, a HIPAA Notice of Privacy Practices was still not posted on Westend Dental's website.

122. Upon information and belief, Westend Dental has never performed a risk assessment that complies with HIPAA. Any "risk assessments" performed by Westend Dental have not accurately reflected the actual policies, practices, or systems of Westend Dental.

Poor Security and Privacy Practices

123. Until at least January 2024, Westend Dental lacked password policies and procedures. Westend Dental allowed employees to share workstation passwords, did not change workstation passwords when employees left the company, and did not regularly change passwords.

124. Before November 2023, Westend Dental lacked any written policies or procedures for updating servers, and there was no set schedule for updating servers.

125. Until at least January 2024, Westend Dental used non-HIPAA-compliant free Gmail accounts to conduct business and transmit and store PHI.

126. Westend Dental's Administrator stored Westend Dental login credentials in a shared, plain text spreadsheet in a Google account.

127. Until at least January 2024, Westend Dental employees used shared email accounts to conduct business, and Westend Dental did keep any record of which employees had access to each email account.

128. Upon information and belief, Westend Dental did not execute a business associate agreement with its billing vendor until April 12, 2023, after the OAG commenced its investigation.

129. Although Kunal Rana was not an employee of Westend Dental, and had never executed a business associate agreement with Westend Dental, Kunal Rana was given access to Westend Dental patient PHI.

130. Finally, until at least October 2023, Westend Dental did not limit physical access to its servers. No servers were stored behind closed doors, and certain servers were stored in common areas such as an employee break room and an employee bathroom.

V. CAUSES OF ACTION

COUNT ONE:
FAILURE TO COMPLY WITH HIPAA BREACH NOTIFICATION RULE
(45. C.F.R. Part 164, Subpart D)

131. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

132. Westend Dental was required to notify patients impacted by the Data Breach "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." 45 C.F.R. § 164.404(b).

133. Westend Dental discovered the Data Breach on October 20, 2020. Accordingly, Westend Dental was required to notify patients affected by the Data Breach no later than December 19, 2020.

134. However, Westend Dental has never provided notification of the Data

Breach to the affected patients.

135. Two years after the Data Breach, Westend Dental submitted a data breach notification form to the OAG indicating the Data Breach affected fewer than 500 individuals, but the actual number of affected patients is unknown and may be much greater because Westend Dental never completed a forensic investigation.

136. At the time of the Data Breach, there was no logging or monitoring of access to Westend Dental databases containing PHI.

137. Further, at the time of the Data Breach, Westend Dental maintained lists of usernames and passwords for systems that contained PHI in plain text files and used the same username and password combination for each of their servers that contained PHI.

138. Upon information and belief, through access to the Arlington Westend Dental server, the Intruder gained access to Westend Dental's shared login credentials stored in plain text files, which gave the Intruder access to all Westend Dental systems and the PHI of all Westend Dental patients.

139. At the time of the Data Breach, Westend Dental served at least 17,000 patients at all locations.

140. Westend Dental's notification to patients is unreasonably delayed and untimely, in violation of 45 C.F.R. § 164.404.

141. Westend Dental's failure to notify patients of the Data Breach is a continuing violation of the HIPAA Breach Notification Rule.

142. The Indiana Attorney General is authorized by 42 U.S.C. § 1320d-5(d)

to bring this action to enjoin such continuing violations and obtain statutory damages of $100 per violation, per day, totaling up $25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

COUNT TWO:
FAILURE TO COMPLY WITH HIPAA SECURITY RULE
(45 C.F.R. Part 164, Subpart C)

143. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

144. For years, Westend Dental failed to employ appropriate safeguards to maintain the security and integrity of PHI, in violation of the HIPAA Security Rule, including as follows:

a. Westend Dental failed to implement, review, and/or modify policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §§ 164.308(a)(1)(i) and 164.306(e);

b. Westend Dental failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by Westend Dental in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);

c. Westend Dental failed to implement a risk management plan with security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B);

d. Westend Dental failed to implement procedures to regularly review

records of information system activity, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

e. Westend Dental failed to implement policies and procedures to ensure that all members of its workforce have appropriate access to PHI and to prevent inappropriate access to PHI in violation of 45 C.F.R. § 164.308(a)(3);

f. Westend Dental failed to implement policies and procedures for authorizing access to PHI consistent with the Privacy Rule in violation of 45 C.F.R. § 164.308(a)(4);

g. Westend Dental failed to implement a security awareness and training program for all members of its workforce, including management, in violation of 45 C.F.R. § 164.308(a)(5);

h. Westend Dental failed to implement procedures for guarding against, detecting, and reporting malicious software, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(B);

i. Westend Dental failed to implement procedures for monitoring log-ins, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(C);

j. Westend Dental failed to implement procedures for creating, changing, and safeguarding passwords, or reasonable and appropriate

alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);

k. Westend Dental failed to implement policies and procedures to address security incidents, and failed to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known; and document security incidents and their outcomes in violation of 45 C.F.R. § 164.308(a)(6);

l. Westend Dental failed to establish and implement procedures to create and maintain retrievable exact copies of PHI in violation of 45 C.F.R. § 164.308(a)(7)(ii)(A);

m. Westend Dental failed to obtain written satisfactory assurances, in accordance with 45 C.F.R. § 164.314(a), that its business associates will appropriately safeguard PHI in violation of 45 C.F.R. § 164.308(b);

n. Westend Dental failed to implement policies and procedures to limit physical access to its electronic information systems in violation of 45 C.F.R. § 164.310(a);

o. Westend Dental failed to implement technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons that have been granted access rights, including assignment of unique names and/or numbers for identifying and tracking user identity in violation of 45 C.F.R. § 164.312(a); and

p. Westend Dental failed to implement hardware, software, and/or

procedural mechanisms that record and examine activity in information systems that contain PHI in violation of 45 C.F.R. § 164.312(b).

145. Each security failure identified in Paragraph 144 is a separate, continuing violation of the HIPAA Security Rule that began before the Data Breach.

146. The Indiana Attorney General is authorized by 42 U.S.C. § 1320d-5(d) to bring this action to enjoin such continuing violations and obtain statutory damages of $100 per violation, per day, totaling up $25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

COUNT THREE:
FAILURE TO COMPLY WITH HIPAA PRIVACY RULE
(45 C.F.R. Part 164, Subpart E) – DISCLOSURES OF PHI

147. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

148. As a covered entity, Westend Dental was prohibited from disclosing PHI except as permitted by HIPAA. 45 C.F.R. § 164.502(a).

149. HIPAA defines "disclosure" as "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 C.F.R. § 160.103.

150. Westend Dental repeatedly disclosed PHI in public replies to online patient reviews and made public posts disclosing PHI and identifying individuals, including minor children, as patients of Westend Dental without patient authorization.

151. Additionally, Westend Dental's poor security practices subjected the PHI of at least 450 Indiana residents to disclosure during the Data Breach.

152. The disclosures were not permitted under any HIPAA exception.

153. Each disclosure violated 45 C.F.R. § 164.502.

154. The Indiana Attorney General is authorized by 42 U.S.C. § 1320d-5(d) to bring this action to obtain statutory damages of $100 per violation, per day, totaling up $25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

COUNT FOUR:
FAILURE TO COMPLY WITH HIPAA PRIVACY RULE
(45 C.F.R. § 164.520) – NOTICE OF PRIVACY PRACTICES

155. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

156. 45 C.F.R. § 164.520 requires covered entities to provide patients with a notice of privacy practices regarding the uses and disclosures of PHI that may be made by the covered entity and the patient's rights and covered entity's legal duties with respect to PHI.

157. 45 C.F.R. § 164.520(c)(3)(i) further provides: "A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site."

158. However, as of December 23, 2024, Westend Dental does not post or make available on its website a notice of privacy practices that contains the

information required by 45 C.F.R. § 164.520 (a "HIPAA Notice of Privacy Practices").

159. For years – and despite the issue being raised in the course of the OAG's investigation – Westend Dental has failed to post or make available on its website a HIPAA Notice of Privacy Practices in violation of 45 C.F.R. § 164.520.

160. The Indiana Attorney General is authorized by 42 U.S.C. § 1320d-5(d) to bring this action to obtain statutory damages of $100 per violation, per day, totaling up $25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

COUNT FIVE:
FAILURE TO IMPLEMENT AND MAINTAIN REASONABLE PROCEDURES IN VIOLATION OF INDIANA DISCLOSURE OF SECURITY BREACH ACT
(Ind. Code § 24-4.9 *et seq*.)

161. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

162. The DSBA defines "data base owner" as "a person that owns or licenses computerized data that includes personal information." Ind. Code § 24-4.9-2-3.

163. The DSBA defines "personal information" to include:

> (1) a Social Security number that is not encrypted or redacted; or
>
> (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
> (A) A driver's license number.
> (B) A state identification card number.
> (C) A credit card number.
> (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Ind. Code § 24-4.9-2-10.

164. The DSBA requires a data base owner to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." Ind. Code § 24-4.9-3-3.5(c).

165. Westend Dental is a data base owner subject to the DSBA.

166. The categories of information exposed by the Data Breach included names and driver's license numbers.

167. Westend Dental violated the DSBA's safeguard requirement by failing to implement and maintain reasonable security procedures to protect and safeguard personal information of Indiana residents.

168. Westend Dental is not exempt from the DSBA because Westend Dental was not in compliance with HIPAA at the times relevant to this Complaint. *See* Ind. Code § 24-4.9-3-3.5(a).

169. Pursuant to Ind. Code § 24-4.9-3-3.5(e) & (f), the Indiana Attorney General may bring an action to obtain a civil penalty of up to $5,000 per deceptive act in violation of the safeguard requirement.

COUNT SIX:
FAILURE TO PROVIDE BREACH NOTIFICATION IN VIOLATION OF INDIANA DISCLOSURE OF SECURITY BREACH ACT
(Ind. Code § 24-4.9 *et seq*.)

170. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

171. Westend Dental is a data base owner subject to the DSBA.

172. The categories of information exposed by the Data Breach included names and driver's license numbers.

173. Westend Dental knew or should have known that the Data Breach could result in identity deception, identity theft or fraud affecting Indiana residents, as provided by Ind. Code § 24-4.9-3-1(a).

174. Westend Dental was required to disclose the Data Breach to affected Indiana residents and the OAG after it discovered the Data Breach "without unreasonable delay," as required by Ind. Code §§ 24-4.9-3-1 and 24-4.9-3-3 (version effective prior to July 1, 2022).

175. Westend Dental unreasonably delayed submitting a data breach notification form to the OAG until October 28, 2022, over two (2) years after Westend Dental discovered the Data Breach.

176. The data breach notification form that Westend Dental eventually submitted falsely stated, "THE INCIDENT WAS NOT OF DATA BREACH."

177. Additionally, the actual number of affected patients is unknown and may be much greater than what Westend Dental indicated on its data breach notification form – fewer than 500 individuals – because Westend Dental never completed a forensic investigation.

178. Westend Dental has never notified patients of the Data Breach.

179. Westend Dental's delay in notifying Indiana residents is not necessary to restore the integrity of the computer system, to discover the scope of the breach, or in response to law enforcement. *See* Ind. Code § 24-4.9-3-3(a).

180. By failing to notify Indiana residents and the OAG of the Data Breach in accordance with Ind. Code §§ 24-4.9-3-1 and 24-4.9-3-3, Westend Dental committed two (2) deceptive acts actionable by the OAG under Ind. Code § 24-4.9-4-1.

181. Pursuant to Ind. Code § 24-4.9-4-2, the Indiana Attorney General may obtain a civil penalty of up to $150,000 for Westend Dental's failure to notify patients.

182. Pursuant to Ind. Code § 24-4.9-4-2, the Indiana Attorney General may obtain a civil penalty of up to $150,000 for Westend Dental's unreasonably delayed notification to the OAG.

COUNT SEVEN:
VIOLATIONS OF INDIANA DECEPTIVE CONSUMER SALES ACT
(Ind. Code § 24-5-0.5 *et seq.*)

183. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

184. The DCSA regulates unfair, abusive, and/or deceptive acts, omissions, and/or practices between suppliers and consumers engaging in consumer transactions. *See* Ind. Code § 24-5-0.5-3.

185. Under the DCSA, a "consumer transaction" includes services and other intangibles. Ind. Code § 24-5-0.5-2(a)(1).

186. In supplying Indiana patients with dental products and services, Westend Dental was and remains involved in consumer transactions in Indiana and is a "supplier" as defined by Ind. Code § 24-5-0.5-2(a)(3).

187. The DCSA prohibits a supplier from committing "an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice

prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code. § 24-5-0.5-3(a).

188. On its website, Westend Dental represents:

a. "Westend Dental is committed to ensuring that your privacy is protected"; and

b. "We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information . . . ."[10]

189. Contrary to these representations, Westend Dental knowingly failed to protect patients' privacy, including by disclosing PHI in public replies to online patient reviews and making public posts disclosing PHI and identifying individuals, including minor children, as patients of Westend Dental without patient authorization.

190. Contrary to these representations, Westend Dental knowingly failed to implement suitable procedures to safeguard and secure patent information, including by failing to implement procedures for secure passwords, access control, or logging and monitoring.

191. Westend Dental's knowing failure to implement reasonable security procedures to protect sensitive patient information and its disclosures of PHI in

[10] *Privacy Policy*, Westend Dental, https://www.mywestenddental.com/disclaimers/privacy/ (last visited Dec. 23, 2024), *accord* Oct. 29, 2020 version, *available at:* https://web.archive.org/web/20201029233659/https://www.mywestenddental.com/disclaimers/privacy/

public replies to online patient reviews and other public posts, without patient authorization, was deceptive, unfair, and abusive in violation of the DCSA.

192. Westend Dental's knowing attempts to cover up the Data Breach by failing to notify patients and making false statements denying that a ransomware attack had occurred were further deceptive, unfair, and abusive in violation of the DCSA.

193. Pursuant to Ind. Code § 24-5-0.5-4(g), the Indiana Attorney General may obtain a civil penalty of up to $5,000 per violation.

194. Westend Dental's attempts to cover up the Data Breach by failing to notify patients and making false statements denying that a ransomware attack had occurred were incurable deceptive acts done as part of a scheme, artifice, or device with intent to defraud or mislead. Ind. Code § 24-5-0.5-2(a)(8).

195. Pursuant to Ind. Code § 24-5-0.5-8, the Indiana Attorney General may obtain additional civil penalties of up to $500 per violation involving an incurable deceptive act.

VI. PRAYER FOR RELIEF

WHEREFORE, the State of Indiana respectfully requests that this Court enter judgment against Westend Dental and in favor of the State as follows:

a. Finding that Westend Dental violated HIPAA, DSBA, and DCSA by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Westend Dental from continuing to engage in such unlawful acts and practices pursuant to 42 U.S.C. § 1320d-5(d)(1)(A), Ind. Code § 24-4.9-3-3.5(f), and

Ind. Code § 24-5-0.5-4(c);

b. Ordering Westend Dental to pay statutory damages of $100 per HIPAA violation, per day, totaling up $25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

c. Ordering Westend Dental to pay a $5,000 civil penalty for violating the safeguard requirement of the DSBA, as provided by Ind. Code § 24-4.9-3-3.5(f);

d. Ordering Westend Dental to pay a $300,000 civil penalty for violating the breach notification requirements of the DSBA, as provided by Ind. Code § 24-4.9-4-2;

e. Ordering Westend Dental to pay a $5,000 civil penalty for each knowing violation of the DCSA alleged herein, as provided by Ind. Code § 24-5-0.5-4(g);

f. Ordering Westend Dental to pay civil penalties of $500 per DCSA violation involving an incurable deceptive act, as provided by Ind. Code § 24-5-0.5-8;

g. Ordering Westend Dental to pay all costs and fees for the investigation and prosecution of this action pursuant to 42 U.S.C. § 1320d-5(d)(3), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c); and

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

Respectfully submitted,

STATE OF INDIANA EX REL.
INDIANA ATTORNEY GENERAL
TODD ROKITA

Date: 12/23/2024

By: /s/ *Jennifer M. Van Dame*

JENNIFER M. VAN DAME
Data Privacy & Identity Theft Unit
Assistant Section Chief
Indiana Bar No. 32788-53
Jennifer.VanDame@atg.in.gov

DOUGLAS S. SWETNAM
Data Privacy & Identity Theft Unit
Section Chief
Indiana Bar No. 15860-49
Douglas.Swetnam@atg.in.gov

302 West Washington Street
IGCS – 5th Floor
Indianapolis, IN 46204
(317) 232-0486 (Van Dame)
(317) 232-6294 (Swetnam)
(317) 232-7979 (Fax)

Counsel for Plaintiff