

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 23-062

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

HEALTHPLEX, INC.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12), General Business Law (“GBL”) §§ 349, 899-aa, and 899-bb, and 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, into a data security incident at Healthplex, Inc. (“Healthplex” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of NYAG’s investigation and the relief agreed to by NYAG and Healthplex.

NYAG FINDINGS

1. On or about November 22, 2021, unknown attacker(s) (the “attacker”) sent a phishing e-mail to a Healthplex employee email account. On November 24, 2021, the attacker gained access to that account, in which over twelve years of emails, some of which contained customer enrollment information was stored.¹

¹ Healthplex is one of the largest third party dental administrators in the state of New York.

2. The attacker obtained the login credentials to the email account when the account owner, who had been employed by Healthplex for over 20 years, responded to phishing email and provided her login credentials. The attacker was then able to gain access to the account by using the company's recently deployed Office 365 web interface, which lacked multi-factor authentication at the time of the attack. Forensic evidence showed that the attacker's unauthorized access to the account began on November 24, 2021 at approximately 06:00:55 CST.

3. On the same day (November 24), Healthplex became aware of suspicious activity when employees reported phishing emails sent by the impacted employee email account. Upon learning of the event, and also on this same day, Healthplex reset the password for the impacted account and Azure account credentials and engaged its security incident response team to investigate the matter. Healthplex's terminated the attacker's access at approximately 11:58 CST.

4. The attacker had access to the account for less than one day, during which time the attacker had access to emails and attachments dating between May 7, 2009 and November 24, 2022. Some of the exposed emails contained member data that included the member's first and last name in combination with one or more of the following data identifiers: member identification number, insurance group name and number, address, date of birth, credit card number, banking information, Social Security number, driver's license number, username and password for the member portal, email address, phone number, data of service, provider name, billing information, procedure codes, diagnosis codes, prescription drug names and plan affiliation.

5. With the system logging available at the time, Healthplex was unable to determine which emails, if any, were opened and if any Private Information or ePHI was exfiltrated. In total, Healthplex provided notice to 89,955 members, including 63,922 New York State residents.

6. Healthplex's investigation found that the phishing email that initiated the attack

contained a link directing recipients to a credential harvesting website where users were requested to enter a username and password to view a PDF file. In response to the incident and the subsequent investigation, Healthplex engaged a third-party eDiscovery firm to review the contents of the compromised email account, comprising nearly 130,000 emails that required some form of review.

7. On April 15, 2022, after receiving a file from the eDiscovery vendor that enabled Healthplex to positively identify impacted members, Healthplex issued notice to the impacted members with the offer of two years of LifeLock Identity Theft Protection Services.

8. Prior to the incident, Healthplex had in place an information security program led by its Chief Information Security Officer. Healthplex's information security program involves policies and procedures designed to safeguard Private Information and ePHI from unauthorized use or disclosure; password management requirements, including requirements for complex passwords; account management/authentication programs, including prohibitions against shared accounts and use of multi-factor authentication; a centralized logging solution designed to collect/monitor network activity; and a penetration testing program. Following the incident, Healthplex took a number of remedial actions, including extending multi-factor authentication to the Office 365 web interface impacted in the phishing attack, a 90-day email retention policy, and additional security training on phishing emails for employees. Healthplex also upgraded its O365 license to obtain enhanced logging capabilities and other security improvements.

9. The NYAG's investigation identified the following areas where Healthplex's practices did not meet the requirements of New York's data security and consumer protection laws:

- a. Data Retention and Logging: The impacted email account contained e-mails/attachments dating back to May 2009 and did not have an email retention policy in place despite the existence of Private Information in employee

mailboxes.² Retention of Private Information after it is no longer needed for business purposes unnecessarily introduces risk of exposure for members. It would be unreasonable to leave Private Information in the affected email account for up to twelve (12) years rather than delete any information if it did not have a business purpose and copy and store any other information in more secure systems and delete the older messages from the affected email account. If retention of such large volumes of email containing member information was a necessary business practice, then Healthplex should have availed itself of better email security and logging capabilities, including multi-factor authentication on all login vectors and system logging that would enable Healthplex's security team to determine which emails from a compromised account have been viewed or otherwise accessed.

- b. Multi-Factor Authentication: Healthplex failed to employ multi-factor authentication across all Office 365 login vectors at the time of the incident, namely the office.com web application.
- c. Data Security Assessments: Healthplex's data security assessments did not identify the vulnerability described above.

10. Based on the foregoing, the NYAG has determined that Healthplex violated Executive Law § 63(12) and GBL §§ 349, 899-aa, and 899-bb.

11. Respondent neither admits nor denies NYAG's Findings, paragraphs 1-10 above.

12. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant

² Healthplex did have in place a general document retention policy outside of e-mail.

to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), and GBL §§ 349, 899-aa, and 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

13. For the purposes of this Assurance, the following definitions shall apply:
 - A. “Effective Date” shall be the date of the last signature to this agreement.
 - B. “Private Information” shall have the same meaning as in GBL § 899-aa(1)(b).
 - C. “ePHI” shall have the meaning set forth in in 45 C.F.R. § 160.103.

GENERAL COMPLIANCE

14. Healthplex shall comply with Executive Law § 63(12), GBL §§ 349, 899-aa, and 899-bb, and HIPAA, in connection with its collection, use, and maintenance of Private Information and ePHI, and shall maintain reasonable security policies and procedures designed to safeguard Private Information and ePHI from unauthorized use or disclosure.

15. Healthplex shall not misrepresent the extent to which Healthplex maintains and protects the privacy, security, confidentiality, or integrity of Private Information and ePHI collected from or about customers.

16. Chief Information Security Officer: Healthplex shall employ a Chief Information Security Officer who must report to Healthplex’s CEO regularly and to Healthplex’s Board of Directors annually.

17. Information Security Program: Healthplex shall maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Private Information and ePHI, including protected health information, that it

collects, receives, or processes.

18. Encryption: Healthplex shall encrypt member Private Information as defined by GBL § 899-aa(1)(b) and ePHI that it collects, stores, transmits and/or maintains, whether stored within the Healthplex computer network, or transmitted electronically within or outside the network, using a reasonable encryption algorithm where technically feasible or otherwise implementing compensating controls to protect such information from unauthorized access.

19. Data Disposal: Healthplex shall dispose of Private Information when there is no business purpose to retain it.

20. Email Retention: Healthplex shall implement a reasonable email retention schedule for all employee email accounts that may contain Private Information or ePHI.

21. Password Management: Healthplex shall maintain reasonable password policies and procedures requiring the use of complex passwords, and ensuring that stored passwords are properly protected from unauthorized access, including, without limitation, hashing stored passwords using a reasonable hashing algorithm and salting policy commensurate with security risks that are known or reasonably should be known.

22. Authentication Policy and Procedures: Healthplex shall maintain reasonable account management and authentication, including forbidding the use of shared user accounts and requiring the use of multi-factor authentication for all administrative or remote access accounts. It shall be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Healthplex's needs and goals.

23. Logging and Security: Healthplex shall maintain a centralized logging solution designed to collect and monitor network activity, including suspicious activity information, console logins and configuration changes. Healthplex shall also implement a security solution that

includes mobile device management and the ability to set rules on how users access and share data on mobile devices. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

24. Penetration Testing: Healthplex shall maintain a reasonable penetration testing program designed to identify, assess, and remediate security vulnerabilities within the Healthplex computer network. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

25. Healthplex previously offered impacted individuals with two (2) years of LifeLock Identity Theft Protection services at no cost. Healthplex shall continue to provide those services for the full two (2) years initially offered and offer the same service to any customers who are subsequently determined to have been impacted by the November 24, 2021 data breach.

26. Healthplex shall pay to the State of New York four hundred thousand dollars (\$400,000.00) in penalties, disgorgement, and costs (the "Monetary Relief Amount"). Payment shall be made payable to the State of New York in full within forty-five (45) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 23-062.

27. The Respondent shall provide NYAG with a certification affirming its compliance with the requirements set forth in this Assurance, paragraphs 13-24, to be submitted to NYAG within sixty (60) days of the Effective Date of this Assurance. This certification shall be in writing and be signed by an officer of Respondent. Thereafter, a certification of compliance shall be submitted to NYAG on an annual basis for the following three (3) years. In any case where the circumstances warrant, NYAG may require Respondent to file an interim certification of compliance upon thirty (30) days notice.

MISCELLANEOUS

28. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 34, and agrees and acknowledges that in the event the Assurance is voided:

a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

29. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

30. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

31. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

32. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

33. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-062, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

Healthplex, Inc
c/o
Kim Peretti, Esq.
Kristy Brown, Esq.
Alston Bird, LLP
The Atlantic Building
950 F Street, NW
Washington, D.C. 20004-1404

If to NYAG, to:

Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

34. NYAG has agreed to the terms of this Assurance based on, among other things, the

representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-10 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any material misrepresentations by Respondent or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

35. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

36. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

37. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

38. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its Effective Date.

39. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

40. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

41. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

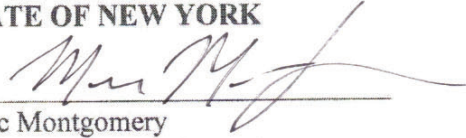
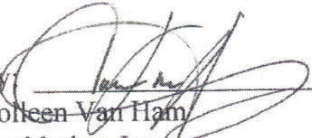
42. This Assurance shall be governed by the laws of the State of New York without

regard to any conflict of laws principles.

43. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

43. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance
have been affixed hereto on the dates set forth below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By:  Marc Montgomery Assistant Attorney General Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p><u>12-8-2023</u> Date</p>	<p>HEALTHPLEX, INC.</p> <p>By:  Colleen Van Ham Healthplex, Inc. Chief Executive Officer 200 E Randolph Street Chicago, IL 60601</p> <p><u>12.7.23</u> Date</p>
--	--