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

In the Matter of

Assurance No. 24-056

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

ENZO BIOCHEM, INC., and
ENZO CLINICAL LABS, INC.,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") § 899-bb into a data security incident at Enzo Biochem, Inc. ("Enzo") and Enzo Clinical Labs, Inc. This Assurance of Discontinuance ("Assurance") contains the findings of the investigation and the relief agreed to by the NYAG and Respondents Enzo and Enzo Clinical Labs, Inc., whether acting through their respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").[1]

NYAG FINDINGS

1. Enzo Biochem, Inc. is a New York-based biotechnology company and the parent company of Enzo Clinical Labs, Inc. Enzo Clinical Labs offered diagnostic testing at laboratories in New York until August 2023, when it sold all laboratory testing assets and exited the clinical

[1] The investigation was conducted with the New Jersey and Connecticut Attorney General offices (collectively, the "Attorneys General") who entered into a similar agreement with Respondents.

laboratory testing business. After the asset sale, Enzo transitioned patient testing information and tissue blocks to an enterprise information management secure storage provider, and decommissioned servers and systems used to store patient information.

The April 2023 Data Security Incident

2. In early April 2023, attackers gained remote access to Enzo's private network. The attackers were then able to move through the network using at least two Enzo user accounts with administrator privileges. The login credentials to two administrator accounts the attackers used were shared among five employees and the credentials associated with one of these accounts had not been changed for ten years.

3. The attackers accessed a variety of Enzo systems and data that contained patient information, including files stored on shared network space, and a database. None of these files or data were encrypted at the file level. The attackers did not access or encrypt with ransomware Enzo's laboratory information system, which contained patient lab results.

4. The attackers also installed malicious software on several Enzo systems. On April 4, this software began pinging attacker-controlled servers outside of the Enzo network. Over the course of two days, the software made hundreds of thousands of attempts to connect to these servers. Enzo's firewall identified tens of thousands of these connection attempts as malicious and blocked them. However, Enzo personnel did not become aware of the attackers' activity until several days later because Enzo did not have a system or process in place to monitor for, or provide notice of, suspicious activity.

5. On April 5, 2023, the attackers exfiltrated Enzo files and data that contained patient information. The attackers also deployed ransomware that encrypted several Enzo systems,

rendering them inaccessible without the decryption key held by the attackers. Enzo discovered the encrypted systems, and the attack, on April 6, 2023.

6. The attackers subsequently provided Enzo with information concerning the systems and data they had accessed, including a listing of hundreds of thousands of files the attackers had exfiltrated, which the attackers claimed comprised approximately 1.4 terabytes of data, some of which contained patient information. The attackers demanded a ransom payment to provide the decryption key to unlock the encrypted files and not publicly release the stolen information.

7. On April 6, 2023, Enzo engaged legal counsel, which engaged a cybersecurity firm to conduct an investigation. The cybersecurity firm was able to find some evidence of the attackers' activity. Enzo provided the cybersecurity firm with logging from the time of the incident, which was limited because Enzo did not maintain comprehensive records of user and network activity. Based on the available evidence, the cybersecurity firm did not identify the attackers' initial vector of attack or the method by which attackers compromised Enzo accounts with administrator privileges.

8. The forensic investigation identified ransomware encryption and the presence of the attacker's tools on an Enzo database server. This server, used strictly for analytic and reporting purposes, contained files relating to tests rendered between October 2012 and April 2023 for approximately 2.4 million patients. The files contained a variety of patient information, including patient names, dates of birth, addresses, phone numbers, Social Security numbers, and medical treatment/diagnosis information. Enzo could not determine whether the attacker accessed these files, but provided notice to these patients, as described below.

9. There was also evidence of file exfiltration from an Enzo file server. To determine

whether the file server contained patient information for individuals not already identified in the records contained on the database server, Enzo utilized a third-party vendor to analyze the files for patient information. Working with the vendor, Enzo identified approximately 14,853 additional patients.

10. Of the approximately 2.4 million total patients impacted in the breach, approximately 1,457,843 were New York residents. For another 309,871 of the 2.4 million impacted patients, Enzo did not have state of residence information; however, all patients underwent testing in New York, New Jersey, or Connecticut. Social Security numbers were accessed or acquired for approximately 405,094 New Yorkers.

11. Enzo began providing notice of the breach to impacted patients on June 5, 2023. The notice listed several types of information that could have been accessed or acquired in the incident, including name, date of service, clinical test information and social security number, but did not disclose that certain patients' address, phone number, date of birth, and gender information were also exfiltrated.

Enzo's HIPAA Security Risk Analysis in November 2021

12. In November 2021, an Enzo vendor issued a report containing its findings from a HIPAA security risk assessment. This was the last HIPAA risk assessment Enzo conducted prior to the attack in April 2023.

13. The vendor identified several risks to Enzo's information systems and provided recommended corrective actions for remediation that were not implemented prior to the data security incident in 2023.

14. For example, the vendor found that Enzo had not documented any of the policies

or procedures required by the HIPAA Security Rule, noting that the vendor's previous review in 2017 had also "found gaps" in Enzo's documentation. The vendor recommended that Enzo create and maintain written security policies and procedures to comply with the Security Rule standards and implementation specifications.

15. The vendor also found that Enzo's process for evaluating potential risks to its information systems was "informal." The vendor recommended that Enzo formalize a process for conducting a regular risk analysis, formally document its risk responses in an appropriate and timely manner, and annually review and update the written security risk analysis report based on changes in Enzo's risk posture.

16. In addition, the vendor found that although Enzo encrypted ePHI in transit and at rest on laptops and phones, some of Enzo's servers and desktop workstations stored ePHI at rest without encryption. The vendor recommended that Enzo "implement a software encryption mechanism to secure ePHI at rest on its equipment" or "if encryption is not reasonable in some situations (i.e. servers)...Enzo document the rationale as to why (e.g. system performance issues or vendor's equipment does not support an encryption mechanism, etc.) and the efforts (e.g. alternative safeguards) in place to mitigate this vulnerability."

17. The vendor also found that Enzo conducted manual reviews of user and network activity for anomalies rather than using automated detection systems, and that Enzo's documentation of its review process "needed improvement." The vendor endorsed Enzo's plan to implement an automated log management solution, which it stated would facilitate the review of audit logs and make it more likely that malicious activity would be caught, and recommended implementing automated network monitoring software, which would help define and manage

reviews. Finally, the vendor recommended Enzo implement a schedule for reviews, including at a minimum weekly or monthly reviews of technical audit log activity for intrusion attempts, and monthly or quarterly of security incident tracking reports.

Enzo's Data Security Program in April 2023

18. In the course of its investigation of the Incident, the NYAG determined that at the time of the attack in April 2023, Enzo's data security program was deficient in several areas. These included:

a. Access Controls and Authentication: Enzo failed to implement and maintain appropriate controls to limit access to sensitive data, including failing to use multi-factor authentication for remote access to email, failing to delete or disable unused accounts, failing to rotate account credentials, sharing account credentials among multiple individuals, and failing to restrict employees' access to only those resources and data necessary for their business functions.

b. Protection of Sensitive Information: Enzo failed to encrypt all sensitive patient data maintained at rest.

c. Audit Controls and Monitoring: Enzo failed to implement appropriate controls for recording, and reviewing records of, user activity on its network.

d. Risk Management and Testing: Enzo failed to regularly conduct appropriate risk management analyses and testing of the security of its systems.

e. Information Security Policies: Enzo failed to adequately maintain and adhere to written policies governing information security, asset management, identity and access management, encryption, risk management, network management, vulnerability

management, and the retention of patient data.

Post Breach Developments

19. In the summer of 2023, Enzo completed the sale of its clinical laboratory testing assets and exited the clinical laboratory business.

20. Enzo has represented that, following the attack, it took steps to improve its data security program, including (i) transitioning tissue blocks and patient test information to an enterprise information management secure storage provider; (ii) decommissioning servers and systems used to store patient information; (iii) upgrading its network firewalls to models and services that employ behavioral based threat intelligence monitoring; (iv) installing an Endpoint Detection and Response (EDR) solution on endpoints, that uses machine learning to detect threats; (v) contracting for an external cybersecurity vendor providing 24/7 Security Operations Center (SOC) services with threat alerts, including monitoring of account activity; (v) implementing two factor authentication for remote access to internal systems; (vi) adopting a cloud-based email system; (vi) increasing password minimum length requirements; (vii) implementing multi-factor authentication for additional systems, including all email accounts; (viii) maintaining enterprise-level licensing for cloud-based email and file sharing services; (ix) implementing a zero-trust segmentation solution that prevents unauthorized communications among workloads and devices, and mitigates unauthorized lateral movement in Enzo's network; (x) adding asset management solutions to help track network connected equipment and systems; (xi) following formalized procurement processes to ensure purchase, license, or subscription of IT assets is vetted and approved based on security due diligence and contractual minimum security requirements and

commitments; (xii) implementing a privileged access management solution; (xiii) deploying software to scan for, identify, and prioritize remediation of vulnerabilities; (xiv) formally adopting updated HIPAA Security Policies and Procedures; and (xv) formally adopting updated general user information and acceptable use of IT assets, IT information security, vulnerability management and remediation, and cybersecurity incident management policies.

The Attorney General's Investigation

21. The NYAG launched an investigation into the circumstances of the data breach in June 2023. Enzo has cooperated with the NYAG's investigation.

Respondent's Violations

22. Enzo Clinical Labs, Inc. is a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA) subject to the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D. Enzo's conduct violated both the HIPAA Security Rule and the Breach Notification Rule, including:

a. § 164.308(a)(1)(i), which requires policies and procedures to prevent, detect, contain, and correct security violations;
b. § 164.308(a)(1)(ii)(A) and (B), which require an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI, and implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a);
c. § 164.308(a)(1)(ii)(D), which requires procedures to regularly review records of information system activity;

d. § 164.308(a)(4)(i), which requires policies and procedures for authorizing access to ePHI;

e. § 164.308(a)(4)(ii)(B) and (C), which require policies and procedures for granting access to ePHI, and establishing, documenting, reviewing, and modifying user's right of access based on access authorization policies;

f. § 164.308(a)(5)(ii)(C) and (D), which require procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords;

g. § 164.308(a)(8), which requires periodic technical and nontechnical evaluations of a covered entity's security policies and procedures;

h. § 164.312(a)(1), (2)(i), and (2)(iv), which require technical policies and procedures for systems that maintain ePHI to allow access to persons granted access rights, unique user identification, and a mechanism to encrypt ePHI;

i. § 164.312(b), which requires controls for recording and examining activity in systems that contain or use ePHI;

j. § 164.312(d), which requires procedures to verify that a person seeking access to ePHI is the one claimed;

k. § 164.316(b), which requires the implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule;

l. § 164.404, which requires notification of individuals whose unsecured PHI is accessed as the result of a breach, including a description of the types of unsecured PHI involved in the breach.

23. Enzo's conduct also violated GBL § 899-bb, which requires implementation and maintenance of reasonable safeguards to protect consumer information.

24. Respondents neither admit nor deny the NYAG's findings, paragraphs 1-23 above.

25. 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

to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of GBL §§ 899-aa and 899-bb, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D.

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

PROSPECTIVE RELIEF

26. For the purposes of this Assurance, the following definitions shall apply:

a. "Consumer" shall mean any person residing in, or who has resided in New York.

b. "Consumer Personal Information" shall mean Private Information and PHI of a Consumer.

c. "Private Information" shall mean private information as defined in New York General Business Law § 899-aa(1)(b).

d. "Protected Health Information" or "PHI" shall mean health information, as defined in section 160.103 of title 45 of the Code of Federal Regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA").

e. "Security Event" shall mean unauthorized access to or acquisition of Consumer Personal Information owned, licensed, or maintained by Respondent.

GENERAL COMPLIANCE

27. Respondents shall comply with GBL § 899-bb, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D in connection with the collection, use, and maintenance of Consumer Personal

Information.

INFORMATION SECURITY PROGRAM

28. Respondents shall maintain a comprehensive Information Security Program that is reasonably designed to protect the security, integrity, and confidentiality of Consumer Personal Information that Respondents collect, store, transmit, destroy, and/or maintain. The Information Security Program shall include the specific information security safeguards set forth in Paragraphs 33 through 43 of this Assurance. The Information Security Program shall adopt, where feasible, principles of zero trust architecture. Respondents shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

a. Assess and document, not less than annually, internal and external risks to the security, integrity, and confidentiality of Consumer Personal Information;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondents identified that are appropriate to: (i) the size and complexity of Respondents' operations; (ii) the nature and scope of Respondents' activities; and (iii) the volume and sensitivity of the Consumer Personal Information that Respondents collect, store, transmit, and/or maintain.

c. Assess and document, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondents identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;

d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;

e. Select service providers capable of appropriately safeguarding Consumer Personal Information, contractually require service providers to implement and maintain appropriate safeguards to protect Consumer Personal Information, and take appropriate steps to verify service providers are complying with the contractual requirements;

f. Evaluate and document, not less than annually, the Information Security Program and adjust the Program in light of any changes to Respondents' operations or business arrangements, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Program.

29. Respondents shall designate a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program. The designated individual shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of the individual's role in implementing, maintaining, and monitoring the Information Security Program. The designated individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management, and shall report at a minimum semi-annually to the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning Respondent's Information Security Program. Such reports shall be in writing and include, but not be limited to, the following: the staffing and budgetary sufficiency

of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by Respondents, and any barriers to the success of the Information Security Program.

30. Respondents shall provide notice of the requirements of the Assurance to their management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. Respondent shall provide security awareness and privacy training to all personnel whose job involves access to or responsibility for Consumer Personal Information. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the effective date of the Assurance, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program or gains access to or responsibility for Consumer Personal Information. Respondents shall provide such training on at least an annual basis. Respondents shall document that they have provided the notices and training required in this paragraph.

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

31. Access and Authentication Controls: Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, policies and procedures to appropriately limit access to Consumer Personal Information that Respondents collect, store, transmit, destroy, and/or maintain. The policies and procedures shall require, at a minimum:

a. Granting individuals and organizations access only to those resources and data that are necessary for their business functions; for the avoidance of doubt, this

subparagraph includes resources and data maintained on a Respondent's network;

b. Promptly removing individuals' and organizations' access to resources and data upon separation, or, upon an individual's change in responsibilities, promptly removing the individual's access to resources and data that are no longer needed to discharge those responsibilities;

c. Prohibiting the use of shared individual user accounts without individualized authentication from each individual; and

d. Conducting an audit, not less than semi-annually, to ensure compliance with these policies.

Notwithstanding the foregoing, Respondents shall be deemed in compliance with subparagraph (c) or (d), if, with respect to the subparagraph, they implement an equivalent, widely adopted industry measure and the person responsible for the Information Security Program: (1) approve(s) in writing the use of such equivalent measure, and (2) documents in writing how the measure is widely adopted and at least equivalent to the security provided by the subparagraph.

32. Account Audit: Within ninety (90) days of the effective date of this Assurance, Respondents shall conduct an audit to ensure compliance with subparagraphs 31(a) and (b).

33. Multi-Factor Authentication: Respondents shall, to the extent they have not already done so, implement, and thereafter maintain multi-factor authentication for all individual user accounts, including system administrator accounts, and for remote access to its computer network.

34. Password Management: Respondent shall, to the extent they have not already done so, establish and implement, and thereafter maintain, policies and procedures requiring the use of

strong, complex passwords and password rotation, and ensuring that stored passwords are properly protected from unauthorized access. Such policies and procedures shall prohibit the use of default, shared, or generic passwords.

35. Encryption: Respondents shall encrypt Consumer Personal Information that they collect, store, transmit, and/or maintain using an encryption method appropriate to the sensitivity of the Consumer Personal Information.

36. Asset Inventory: Respondents shall maintain and regularly update an inventory that appropriately identifies all assets containing Consumer Personal Information.

37. Risk Assessment Program: Respondents shall conduct annual risk assessments, which shall include identification of all reasonably anticipated internal and external risks to the security, confidentiality, or integrity of Consumer Personal Information. The results of the risk assessment shall be documented, and such documentation shall be maintained by the designated individuals referenced in Paragraph 29 of this Assurance and be available for inspection by the third-party assessor described in Paragraph 44 of this Assurance.

38. Penetration Testing: Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, a penetration testing program designed to identify, assess, and remediate security vulnerabilities within Respondents' environments. Testing shall occur on at least an annual basis. The results of the testing, assessment, and remediation shall be documented, and such document shall be maintained by the designated individual referenced in Paragraph 29 of this Assurance and be available for inspection by the third-party assessor described in Paragraph 44 of this Assurance.

39. Segmentation: Respondents shall, to the extent they have not already done so,

establish and implement, and thereafter maintain, policies and procedures designed to properly segment their networks and ensure that communication between partitions is permitted only to the extent necessary to meet business and/or operational needs.

40. Data Loss/Exfiltration Prevention: Respondents shall, to the extent they have not already done so, implement, and thereafter maintain, a reasonable data loss prevention technology to detect and prevent unauthorized data exfiltration from their networks.

41. Monitoring and Logging: Respondents shall, to the extent they have not already done so, implement, and thereafter maintain, controls to log and monitor all security and operational activity related to Respondents' networks, systems, and assets. The controls shall, at a minimum: (i) provide for centralized logging that includes collection and aggregation of logging for Respondents' networks and any platforms or applications operated by or on behalf of Respondents that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Consumer Personal Information, and (ii) use automated processes to monitor for and alert security personnel to anomalous activity. Respondents shall also establish and maintain policies and procedures to regularly review appropriate records for anomalous activity. Respondents shall store logs of events that indicate anomalous activity for a period of time that is sufficient to detect, investigate, and respond to security incidents.

42. Intrusion Detection and Prevention (IDS/IPS) Solution: Respondents shall, to the extent they have not already done so, implement, and thereafter maintain, reasonable intrusion detection and prevention (IDS/IPS) systems designed to detect and prevent unauthorized access to its environment.

43. Endpoint Detection and Response (EDR) Solution: Respondents shall, to the extent

they have not already done so, implement, and thereafter maintain, current, up-to-date endpoint detection and response (EDR) solutions or software on their networks, which shall be at the highest technical level available.

INFORMATION SECURITY PROGRAM ASSESSMENTS

44. Within one hundred and eighty (180) days of the effective date of this Assurance, Respondents shall obtain a comprehensive assessment of the information security of Respondents' networks conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Assessment Report") and provided to the NYAG within two weeks of completion. Annually for three (3) years thereafter, Respondents shall obtain Third-Party Assessment Reports which Respondents shall maintain for six (6) years from the date of each Third-Party Assessment Report and shall provide to the NYAG upon request. The third-party assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA), or a similarly qualified person or organization; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security. The Third-Party Assessment Reports shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by Respondents' Information Security Program;

b. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering Respondents' size and complexity, the nature and scope of Respondents' activities, the sensitivity of the Consumer

Personal Information maintained on the networks and the reasonably anticipated risks;

c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondents meet the requirements of the Information Security Program and the Assurance; and

d. Make recommendations to enhance data security measures.

POLICIES

45. Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, reasonable written policies and procedures that govern asset management, identity and access management, encryption, risk management, network management, vulnerability management.

46. Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, policies and procedures governing its collection, use, retention, and disposal of Consumer Personal Information. Respondents shall securely dispose of Consumer Personal Information when there is no business or legal reason to retain such Consumer Personal Information. In particular, these policies and procedures shall:

a. identify responsible team members for accountability;
b. define the applicable data;
c. identify clear disposal requirements and criteria;
d. identify the areas where PI data may be stored;
e. identify data retention standards for such files; and
f. identify related and dependent processes.

INCIDENT RESPONSE

47. Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following:

a. If a Respondent has reason to believe a Security Event has occurred, Respondent shall promptly conduct a reasonable investigation to determine, at a minimum, whether Consumer Personal Information was accessed or acquired without authorization, and, if so, what Consumer Personal Information was accessed or acquired.

b. If the Respondent determines Consumer Personal Information has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondent shall expediently provide each Consumer whose Personal Information has been, or is reasonably believed to have been, accessed or acquired without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the Security Event that is reasonably individualized to the customer including, at a minimum, the timing of the Security Event, whether the Consumer's Personal Information was accessed or acquired without authorization, what Personal Information was accessed or acquired, and what actions have been taken to protect the Consumer. If necessary in order to provide expedient notice to Consumers, Respondent may provide more than one notice that collectively provide all material information.

OAG ACCESS TO RECORDS

48. Respondents shall retain the documentation and reports required by paragraphs 28 through 47 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any other claim.

CREDIT MONITORING

49. Respondents shall offer identity theft protection services to all Consumers whose Private Information was accessed or acquired in the 2023 Security Events and were not previously offered identity theft protection services.

MONETARY RELIEF

50. Respondents shall pay to the Attorneys General Four Million Five Hundred Thousand dollars ($4,500,000.00). Payment shall be made in full within forty-five (45) days of the effective date of this Assurance. Said payments shall be divided and paid by Respondents directly to each of the Attorneys General in an amount designated by the Attorneys General.

51. Payments to the NYAG may be used for any purpose, including without limitation, penalties, costs, attorneys' fees, or any other purpose permitted by New York law, at the NYAG's sole discretion. Payments shall be made by wire in accordance with instructions provided by a NYAG representative and shall reference Assurance No. 24-056.

MISCELLANEOUS

52. Respondents expressly agree and acknowledge 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 59, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 59:

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 Respondents 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 Respondents irrevocably and unconditionally waive 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).

53. If a court of competent jurisdiction determines that a 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.

54. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by Respondent.

55. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of a 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. Notwithstanding the forgoing, nothing herein waives or limits any immunity, supremacy or other authority applicable or assertable by or on behalf of the federal government or any agency thereof.

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

57. Any failure by the NYAG to insist upon the strict performance by a 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.

58. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-056, 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 Enzo, to:

Kimberly Gordy, Partner
Baker & Hostetler, LLP
811 Main Street
Suite 1100
Houston, TX 77002-6111
kgordy@bakerlaw.com

If to Respondent Enzo Clinical Labs, Inc., to:

Kimberly Gordy, Partner
Baker & Hostetler, LLP
811 Main Street

Suite 1100
Houston, TX 77002-6111
kgordy@bakerlaw.com

If to NYAG, to:

Jordan Adler, Senior Enforcement Counsel, or in his absence,
to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
jordan.adler@ag.ny.gov

59. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and their counsel and NYAG's own factual investigation as set forth in the Findings, paragraphs 1-21 above. Respondents represent and warrant that neither they nor their counsel have made any material representations to NYAG that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or misleading, this Assurance is voidable by NYAG in its sole discretion.

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

61. Respondents represent and warrant, through the signature below, that the terms and conditions of this Assurance are duly approved.

62. Respondents agree not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondents' right to take legal or factual positions in defense of litigation or other legal proceedings to which

the NYAG is not a party.

63. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that a Respondent violates the Assurance after its effective date.

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

65. 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.

66. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

67. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

68. 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.

69. 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. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all

matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

70. The effective date of this Assurance shall be August 8, 2024.

LETITIA JAMES **ATTORNEY GENERAL OF** **THE STATE OF NEW YORK** By: /s Jordan Adler Jordan Adler Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 Fax: (212) 416-8369 08/13/24 Date	**ENZO BIOCHEM, INC.** By: Kara Cannon Kara Cannon, Chief Executive Officer 08/08/24 Date **ENZO CLINICAL LABS, INC.** By: Kara Cannon Kara Cannon, Chief Executive Officer 08/08/24 Date