

**FILED**

August 13 2024

Division of Consumer Affairs

ATTORNEY GENERAL OF NEW JERSEY  
Division of Law  
124 Halsey Street, 5th Floor  
P.O. Box 45029  
Newark, New Jersey 07101  
Attorney for the New Jersey Division of Consumer Affairs

By: Kashif T. Chand  
Deputy Attorney General  
(973) 648- 2052

STATE OF NEW JERSEY  
DEPARTMENT OF LAW AND PUBLIC  
SAFETY DIVISION OF CONSUMER AFFAIRS

In the Matter of

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

Respondents.

Administrative Action

**CONSENT ORDER**

**WHEREAS** this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection (the “Division”), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -229 (“CFA”) and/or 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, and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 to 180 (collectively, “HIPAA”) have been or are being committed (the “Investigation<sup>1</sup>”) by ENZO BIOCHEM, INC. (“Enzo”) and ENZO CLINICAL LABS, INC.

<sup>1</sup> The investigation was conducted with the New York and Connecticut Attorney General Offices (collectively, the “Attorneys General”). The Attorney Generals entered into similar agreements with Respondents.

(“Enzo Clinical Labs”) (collectively, the “Respondents”);

**WHEREAS** the Attorney General is charged with the responsibility of enforcing the CFA and the Director of the Division of Consumer Affairs is charged with administering the CFA on behalf of the Attorney General;

**WHEREAS** the Attorney General, as *parens patriae* for the State of New Jersey and in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA;

**WHEREAS** Enzo is a New York-based company incorporated in New York, and headquartered at 60 Executive Boulevard, Farmingdale, NY 11735;

**WHEREAS** Enzo Clinical Labs was a New York-based company incorporated in New York, and headquartered at 60 Executive Boulevard, Farmingdale, NY 11735;

**WHEREAS** Enzo has substantial contacts with New Jersey and provides healthcare services to New Jersey residents;

**WHEREAS** Enzo Clinical Labs had substantial contacts with New Jersey and provided diagnostic testing services to New Jersey and Connecticut residents;

**WHEREAS** the Division alleges that Respondents engaged in conduct that violated the CFA and HIPAA in connection with the unreasonable security measures implemented to secure Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information stored on its private network in or about April 2023, affecting approximately 2,400,000 consumers nationwide, including 331,600 New Jersey residents;

**WHEREAS** the Division alleges that Respondents engaged in conduct that violated the CFA and HIPAA in connection with the improper disclosure of Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information discovered in early April 2023, affecting 2,400,000 consumers nationwide, including 331,600 New Jersey residents;

and

**WHEREAS** the Division and Respondents (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and Respondents having cooperated with the Investigation and consented to the entry of the within order (“Consent Order”) without admitting any violation of law, and for good cause shown;

**IT IS ORDERED AND AGREED** as follows:

**DEFINITIONS**

1. For the purposes of this Consent Order, the following definitions shall apply:
  - a. “Consumer” shall mean any person residing in, or who has resided in New Jersey.
  - b. “Consumer Personal Information” shall mean Private Information and PHI of a Consumer.
  - c. “NJAG” shall refer to the Attorney General of the State of New Jersey and the Office of the Attorney General of the State of New Jersey, inclusive of the Division.
  - d. “Private Information” shall mean the data elements in the definition of personal information set forth in the Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166.3.
  - e. “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”).

- f. “Security Event” shall mean unauthorized access to or acquisition of Consumer Personal Information owned, licensed, or maintained by Respondents.

## **FINDINGS**

2. 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 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

3. In early April 2023, attackers gained remote access to the Respondents’ private network. The attackers were then able to move through the network using at least two of the Respondents 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.

4. The attackers accessed a variety of the Respondents’ 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 the Respondents’ laboratory information system, which contained patient lab results.

5. The attackers also installed malicious software on several the Respondents’ systems. On April 4, this software began pinging attacker-controlled servers outside of the Respondents’ network. Over the course of two days, the software made hundreds of thousands of attempts to connect to these servers. The Respondents’ firewall identified tens of thousands of these connection

attempts as malicious and blocked them. However, Respondents personnel did not become aware of the attackers' activity until several days later because Respondents did not have a system or process in place to monitor for, or provide notice of, suspicious activity.

6. On April 5, 2023, the attackers exfiltrated the Respondents' files and data that contained patient information. The attackers also deployed ransomware that encrypted several Respondents' systems, rendering them inaccessible without the decryption key held by the attackers. The Respondents discovered the encrypted systems, and the attack, on April 6, 2023.

7. The attackers subsequently provided Respondents 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.

8. On April 6, 2023, Respondents 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. Respondents provided the cybersecurity firm with logging from the time of the incident, which was limited because Respondents 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 Respondents' accounts with administrator privileges.

9. The forensic investigation identified ransomware encryption and the presence of the attacker's tools on the Respondents' 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. Respondents could not determine whether the attacker accessed these files, but provided notice to these patients, as described below.

10. There was also evidence of file exfiltration from the Respondents' file server. To determine whether the file server contained patient information for individuals not already identified in the records contained on the database server, Respondents utilized a third-party vendor to analyze the files for patient information. Working with the vendor, Respondents identified approximately 14,853 additional patients.

11. Of the approximately 2.4 million total patients impacted in the breach, approximately 331,600 were New Jersey residents. For another 309,871 of the 2.4 million impacted patients, Respondents 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 109,200 New Jersey residents.

12. Respondents 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.

#### Respondents' HIPAA Security Risk Analysis in November 2021

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

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

15. For example, the vendor found that Respondents 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 the Respondents' documentation. The vendor recommended that Respondents create and maintain written security policies and procedures to comply with the Security Rule standards and implementation specifications.

16. The vendor also found that Respondents' process for evaluating potential risks to its information systems was "informal." The vendor recommended that Respondents 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 Respondents' risk posture.

17. In addition, the vendor found that although Respondents encrypted ePHI in transit and at rest on laptops and phones, some of Respondents' servers and desktop workstations stored ePHI at rest without encryption. The vendor recommended that Respondents "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."

18. The vendor also found that Respondents conducted manual reviews of user and network activity for anomalies rather than using automated detection systems, and that Respondents' documentation of its review process "needed improvement." The vendor endorsed

Respondents' 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 Respondents 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.

#### Respondents' Data Security Program in April 2023

19. In the course of its investigation of the Incident, the NJAG determined that at the time of the attack in April 2023, Respondents' data security program was deficient in several areas.

These included:

- a. Access Controls and Authentication: Respondents 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: Respondents failed to encrypt all sensitive patient data maintained at rest.
- c. Audit Controls and Monitoring: Respondents failed to implement appropriate controls for recording, and reviewing records of, user activity on its network.
- d. Risk Management and Testing: Respondents failed to regularly conduct appropriate risk management analyses and testing of the security of its systems.
- e. Information Security Policies: Respondents 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

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

21. Respondents have 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 utilize machine learning to detect potential threats; (v) contracting with an external cybersecurity vendor that provides 24/7 Security Operations Center (“SOC”) services with threat alerts, including accounting monitoring activity; (vi) implementing two factor authentication for remote access to internal systems; and (vii) adopting cloud-based email system; (ix) increasing password minimum length requirements; (x) implementing multi-factor authentication for additional systems, including all accounts; (xi) maintaining enterprise-level licensing for cloud-based email and file sharing services; (xii) implementing a zero-trust segmentation solution that prevents unauthorized communications among workloads and devices, and mitigates unauthorized lateral movement in Respondents’ network; (xiv) adding asset management solutions to help track network connected equipment and systems; (xv) 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; (xvi) implementing a privileged access management solution; (xvii) deploying software to scan for, identify, and prioritize remediation of vulnerabilities; (xviii) formally adopting updated HIPAA Security Policies and Procedures; and (xix) 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

22. The NJAG launched an investigation into the circumstances of the data breach in June 2023. Respondents have cooperated with the NJAG's investigation.

#### **RESPONDENTS' VIOLATIONS**

23. Respondents are each a "covered entity" under HIPAA. Respondents' 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.

24. Respondents' failure to ensure the proper security of Respondents' Network, affecting the Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information of approximately 2,400,000 consumers nationwide, including 331,600 New Jersey residents, constitutes separate and additional violations of the CFA, N.J.S.A. 56:8-2.

25. Respondents neither admit nor deny the NJAG's findings, paragraphs 2-22 above.

26. The NJAG finds the relief and agreements contained in this Consent Order appropriate and in the public interest. THEREFORE, the NJAG is willing to accept this Consent Order in lieu of commencing a proceeding for violations of the CFA and HIPAA.

## **GENERAL COMPLIANCE**

27. Respondents shall comply with the CFA and HIPAA 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 31 through 44 of this Consent Order. 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; and
- 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 Respondents' 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 Consent Order to their management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. Respondents 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 Consent Order, 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 the Respondents' 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 Consent Order, 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: Respondents 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 document, and such documentation shall be maintained by the designated individuals referenced in Paragraph 29 of this Consent Order and be available for inspection by the third-party assessor described in Paragraph 44 of this Consent Order.

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 Consent Order and be available for inspection by the third-party assessor described in Paragraph 44 of this Consent Order.

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 Consent

Order, 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 NJAG 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 NJAG 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 of 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 Consent Order; 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, identify 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 the Respondents have reason to believe a Security Event has occurred, Respondents 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 Respondents determine Consumer Personal Information has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondents 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 Jersey 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, Respondents may provide more than one notice that collectively provide all material information.

#### **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 NJAG within fourteen (14) days of a written request from the NJAG. 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) in penalties and costs. Payment shall be made in full within forty-five (45) days of the effective date of this Consent Order. Said payments shall be divided and paid by Respondents directly to each of the Attorneys General in an amount designated by the Attorneys General. Upon making the Settlement Payment, Respondents shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the State pursuant to the terms herein. The payment received by the NJAG may be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or may be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education or redress, litigation or local consumer aid fund or revolving fund, used to defray the costs of inquiry leading hereto, and/or for other uses permitted by New Jersey law at the sole discretion of the NJAG.

51. Payments to the NJAG shall be made by wire in accordance with instructions provided by the NJAG.

### **MISCELLANEOUS**

52. Respondents expressly agree and acknowledge that NJAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Consent Order, for violations of the Consent Order, or if the Consent Order is voided pursuant to paragraph 59, and agrees and acknowledges that in the event the Consent Order 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 Consent Order;

- b. the NJAG may use statements, documents or other materials produced or provided by Respondents prior to or after the effective date of this Consent Order; and
- c. any civil action or proceeding must be adjudicated by the courts of the State of New Jersey, and that Respondents irrevocably and unconditionally waive any objection based upon personal jurisdiction, inconvenient forum, or venue.

53. If a court of competent jurisdiction determines that Respondents have violated the Consent Order, Respondents shall pay to the NJAG the reasonable cost, if any, of obtaining such determination and of enforcing this Consent Order, including without limitation legal fees, expenses, and court costs.

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

55. All terms and conditions of this Consent Order shall continue in full force and effect on any successor, assignee, or transferee of the Respondents. Respondents shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Consent Order. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Consent Order without the prior written consent of NJAG. Notwithstanding the forgoing, nothing herein waives or limits any immunity, supremacy or other authority applicable or assertible 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 NJAG to insist upon the strict performance by the Respondents

of any of the provisions of this Consent Order shall not be deemed a waiver of any of the provisions hereof, and the NJAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Consent Order to be performed by the Respondents.

58. All notices, reports, requests, and other communications pursuant to this Consent Order 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:

For Respondents, to:

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

If to NJAG, to:

Kashif T. Chand, Deputy Attorney General  
Office of the Attorney General  
Department of Law and Public Safety  
124 Halsey Street, 5th Floor  
Newark, New Jersey 07101  
Kashif.Chand@law.njoag.gov

59. NJAG has agreed to the terms of this Consent Order based on, among other things, the representations made to NJAG by Respondents and their counsel and NJAG's own factual investigation as set forth in the Findings, paragraphs 2-22 above. Respondents represent and warrant that neither they nor their counsel have made any material representations to NJAG that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or misleading, this Consent Order is voidable by NJAG in its sole discretion.

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

61. Respondents represent and warrant, through the signature below, that the terms and conditions of this Consent Order 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 Consent Order or creating the impression that the Consent Order 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 NJAG is not a party.

63. Nothing contained herein shall be construed to limit the remedies available to NJAG in the event that Respondents violate the Consent Order after its effective date.

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

65. In the event that any one or more of the provisions contained in this Consent Order 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 NJAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

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

67. This Consent Order shall be governed by the laws of the State of New Jersey without regard to any conflict of laws principles.

68. The Consent Order 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 Consent Order 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 Consent Order, all of which shall constitute one agreement to be valid as of the effective date of this Consent Order. For purposes of this Consent Order, 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 Consent Order 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 Consent Order shall be August 8, 2024.

**[SIGNATURE PAGES TO FOLLOW]**

IT IS ON THE 13th DAY OF August, 2024 SO ORDERED.


MATTHEW J. PLATKIN  
ATTORNEY GENERAL OF NEW JERSEY

By: Cari Fais  
CARI FAIS, ACTING DIRECTOR  
DIVISION OF CONSUMER AFFAIRS

**THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS  
CONSENT ORDER ON THE DATES ADJACENT TO THEIR RESPECTIVE  
SIGNATURES.**

**FOR THE DIVISION:**

MATTHEW J. PLATKIN  
ATTORNEY GENERAL OF NEW JERSEY

By:  \_\_\_\_\_

Kashif T. Chand  
Deputy Attorney General  
124 Halsey Street, 5th Floor  
Newark, New Jersey 07101

Dated: 8/13/2024

**ENZO BIOCHEM, INC.:**

By: Kara Cannon  
Kara Cannon, Chief Executive Officer

Dated: 08/08/24, 2024

**ENZO CLINICAL LABS, INC.:**

By: Kara Cannon  
Kara Cannon, Chief Executive Officer

Dated: 08/08/24, 2024