UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MARK GUTHART on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS, Defendants.	:	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff MARK GUTHART ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS ("Enzo Biochem", "Enzo Clinical", and "Labcorp" or, collectively, "Defendants") on behalf of himself individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This Class Action arises from a breach of sensitive information in the possession and custody and/or control of Defendants (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, dates of service, ("personal identifying information" or "PII"), and clinical test information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. According to a letter received by Plaintiff from Defendants, the Data Breach occurred between April 4, 2023, and April 6, 2023. Defendants advise they became aware of the Data Breach on April 6, 2023. Accordingly, cybercriminals had unrestricted and unrestrained access to Plaintiff's and the Class's highly private Sensitive Information for perhaps as long as two days. Discovery may reveal that this occurred for a longer period of time.

4. Defendants sent Plaintiff a letter on June 1, 2023 ("Notice Letter") to inform him of the Data Breach. Thus, Defendants inexplicably waited almost two months before informing Class Members of the Data Breach, even though Plaintiff and the Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Defendants' Breach Notice failed to tell its consumers how many people were impacted, how the breach happened, or why it took Defendants nearly two months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

6. News reporting indicates that approximately 2.5 million individuals were impacted by the Data Breach.[1]

7. Defendants' failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

8. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

[1] https://www.securityweek.com/enzo-biochem-ransomware-attack-exposes-information-of-2-5m-individuals/ (Last Accessed on June 13, 2023).

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to timely adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of their consumers.

10. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures and have been damaged as detailed herein.

11. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

12. Plaintiff, Mark Guthart, is a natural person and citizen of New York, residing in Plainview, New York, where he intends to remain.

13. Defendant Enzo Biochem is a New York Corporation, with its principal place of business at 81 Executive Blvd. Suite 3, Farmingdale, NY, United States, 11735.

14. Defendant Enzo Clinical, is a New York Corporation, with its principal place of business at 28 Liberty Street, New York, NY, United States, 10005.

15. Defendant Labcorp is a North Carolina Corporation, with its principal place of business at 531 South Spring Street, Burlington, NC, United States, 27215.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the

proposed class.

17. This Court has personal jurisdiction over Defendant Enzo Biotech because Defendant maintains its principal place of business in this District and does substantial business in this District.

18. This Court has personal jurisdiction over Defendant Enzo Clinical because Defendant does substantial business and has substantial contacts in this District.

19. This Court has personal jurisdiction over Defendant Labcorp because Defendant does substantial business and has substantial contacts in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

21. Defendant Enzo Clinical is "a full service clinical reference laboratory." [2]

22. As part of their business, Defendants receive and maintain the Sensitive Information of thousands of consumers. In doing so, Defendants implicitly promise to safeguard their Sensitive Information.

23. On information and belief, Defendant Labcorp purchased Defendant Enzo Clinical on March 17, 2023.

24. In collecting and maintaining consumers' Sensitive Information, Defendants agree to safeguard the data in accordance with state and federal law.

25. On information and belief, Defendants have not implemented reasonably cybersecurity safeguards or policies to protect their consumers' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of

[2] https://www.enzoclinicallabs.com/ (Last visited on June 13, 2023).

its systems. As a result, Defendants leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

The Data Breach

26. Defendants collect and maintain consumers' Sensitive Information in its computer systems.

27. On or about April 6, 2023, Defendants became aware that their network may have been breached.

28. Following a forensic investigation, Defendants then discovered that cybercriminals had—between April 4, 2023 and April 6, 2023—accessed a set of electronically stored personal information stored on their network.

29. Defendants' Notice of Data Breach admits that Plaintiff's and Class Members' Sensitive Information was accessed without authorization.[3]

30. In collecting and maintaining Sensitive Information, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies, as well as state and federal law.

31. According to the Breach Notice, on April 6, 2023, Defendants identified a ransomware incident on its computer network, and an investigation determined that an unauthorized party accessed files on its systems between April 4, 2023, and April 6, 2023.

32. Defendants' investigation revealed that their cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private Sensitive Information.

[3] https://www.enzoclinicallabs.com/Uploaded/Website-Notice.pdf (Last Accessed June 13, 2023).

33. On June 1, 2023, nearly two months after the Breach first occurred, Defendants finally began notifying Plaintiff and Class Members about the Data Breach.

34. Through their Breach Notice, Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.

35. On information and belief, Defendants have offered two years complimentary credit monitoring and identity monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

36. Even with two years' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

37. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over their consumers' Sensitive Information. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

38. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and healthcare adjacent industry preceding the date of the breach.

39. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

40. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[4]

41. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendants.

Plaintiff Guthart's Experience

42. As a requisite to receiving medical services from Defendants, Plaintiff provided his Sensitive Information to Defendants and trusted that the information would be safeguarded according to state and federal law. Upon receipt, Sensitive Information was entered and stored in Defendants' network and systems.

43. Plaintiff is very careful about sharing his Sensitive Information, and he has never knowingly transmitted unencrypted Sensitive Information.

44. Plaintiff stores any documents containing his Sensitive Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendants failed to follow basic industry security standards and failed to implement systems to protect his Sensitive Information, he would not have provided that information to Defendants.

[4] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of- targeted-ransomware (last visited June 13, 2023).

45. The Breach Notice dated June 1, 2023 from Defendants notified Plaintiff that their network had been accessed and Plaintiff's Sensitive Information was involved in the Data Breach, which included Plaintiff's name, Social Security Number, dates of service, and clinical test information.

46. Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendants' direction by way of the Data Breach notice where Defendants advised Plaintiff to mitigate his damages by, among other things, reviewing his healthcare statements for accuracy.

47. Even with the best response, the harm caused to Plaintiff cannot be undone.

48. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

49. He also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

50. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

51. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

52. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

53. Plaintiff has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Have Been Injured

54. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

55. As a result of Defendants carelessness, recklessness, negligence and inadequacy, Plaintiff's and Class Members' Sensitive Information has been compromised and they now face an ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves. The exposed Sensitive Information of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web.

56. In addition to the ongoing risk of identity theft, those impacted by the Data Breach have suffered numerous actual and concrete injuries and damages, including:

a. invasion of privacy;

b. financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft;

c. loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk;

d. financial "out of pocket" costs incurred due to actual identity theft;

e. loss of time incurred due to actual identity theft;

f. loss of time due to increased spam and targeted marketing emails;

g. the loss of benefit of the bargain (price premium damages);

h. diminution of value of their Sensitive Information;

i. anxiety, annoyance and nuisance, and

j. the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

k. The loss of the opportunity to control how their Sensitive Information is used;

l. The compromise and continuing publication of their Sensitive Information;

m. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; and

n. Delay in receipt of tax refund monies.

Defendants failed to adhere to FTC guidelines.

57. In 2016, the Federal Trade Commission ("FTC") updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

58. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

59. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

62. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[5]

[5] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of

63. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[6]

64. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that they create, receive, maintain and transmit in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

birth, Social Security numbers, and medical record numbers.

[6] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

65. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Failed to Comply with Industry Standards

66. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

67. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without

a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

68. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

69. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees.

71. Upon information and belief, Defendants failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

72. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

Nationwide Class: All individuals residing in the United States whose Sensitive Information was compromised in the Defendants' Data Breach including all those who received notice of the breach.

73. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

74. Plaintiff reserves the right to amend the class definition.

75. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at approximately 2.5 million members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

76. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

77. Plaintiff realleges all previous paragraphs as if fully set forth below.

78. Plaintiff and members of the Class entrusted their Sensitive Information to Defendants.

79. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

80. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

81. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

82. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's Sensitive Information.

83. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information.

84. Sensitive Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

85. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

86. Defendants' breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

87. Plaintiff realleges all previous paragraphs as if fully set forth below.

88. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

89. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's Sensitive Information.

90. Defendants breached their duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

91. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

92. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

93. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

94. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

95. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

96. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

97. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

98. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

99. Had Plaintiff and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendants with their Sensitive Information.

100. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

101. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges;

loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

102. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class)

103. Plaintiff realleges all previous paragraphs as if fully set forth below.

104. Plaintiff and Class Members were required to provide their Private Information to Defendants as a condition of their use of Defendants' services.

105. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their Private Information from unauthorized access and disclosure.

106. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private

Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

107. When Plaintiff and Class Members provided their PII and PHI to Defendants, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

108. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

109. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure, including monitoring its computer systems and networks to ensure that it adopted reasonable data security measures.

110. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

111. Defendants breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

112. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

113. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide and continue to provide adequate credit monitoring to all Class Members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

115. Plaintiff realleges all previous paragraphs as if fully set forth below.

116. In providing their Private Information to Defendants, Plaintiff and Class Members justifiably placed a special confidence in Defendants to act in good faith and with due regard for the interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

117. Defendants accepted the special confidence Plaintiff and Class Members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff' personal information as included in the Data Breach notification letter.

118. In light of the special relationship between Defendants, Plaintiff, and Class Members, whereby Defendants became a guardian of Plaintiff and Class Members' Private Information, Defendants became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members for the safeguarding of Plaintiff and Class Members' Private Information.

119. Defendants has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers.

120. Defendants breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff' and Class Members' Private Information.

121. Defendants breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff and Class Members' Private Information.

122. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of their Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. The continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

g. The diminished value of the services they paid for and received.

123. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members will suffer other forms of injury and/or harm, and other economic

and non-economic losses.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges all previous paragraphs as if fully set forth below.

125. Plaintiff and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

126. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the services and goods they sold to their consumers, including Plaintiff's and the Class.

127. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

128. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Violation Of The New York Deceptive Trade Practices Act
("GBL") (New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and the Class)

129. Plaintiff realleges all previous paragraphs as if fully set forth below.

130. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus.

Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Sensitive Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of their privacy and security protections for Class Members' Sensitive Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

131. Defendants knew or should have known that their network and data security practices were inadequate to safeguard the Class Members' Sensitive Information entrusted to it, and that the risk of a data breach or theft was highly likely.

132. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

133. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendants' network and aggregation of Sensitive Information.

134. The representations upon which consumers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of Sensitive Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

135. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

136. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Sensitive Information and that the risk of a data security incident was high.

137. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York.

138. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Sensitive Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

139. As a direct and proximate result of Defendants' multiple, separate violations of GBL §349, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

140. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

141. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

142. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, in junctive relief, and/or attorney's fees and costs.

143. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

144. Also as a direct result of Defendants' violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VII
Declaratory and Injunctive Relief
(On Behalf of Plaintiff and the Class)

145. Plaintiff realleges all previous paragraphs as if fully set forth below.

146. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, et seq.

147. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

148. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Sensitive Information, and whether Defendants is currently

maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Sensitive Information. Plaintiff and the Class remain at imminent risk that further compromises of their Sensitive Information will occur in the future.

149. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect employee and patient Sensitive Information.

150. Defendants still possess the Sensitive Information of Plaintiff and the Class.

151. To Plaintiff's knowledge, Defendants have made no announcement that it has changed their data storage or security practices relating to the Sensitive Information, beyond the vague claim in the Data Breach Letter that it is "[taking] steps to enhance the security of our computer systems and the data we maintain."

152. To Plaintiff's knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

153. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Enzo. The risk of another such breach is real, immediate, and substantial.

154. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Sensitive Information and Defendants' failure to address the security failings that led to such exposure.

155. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

156. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Enzo, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

157. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Enzo, thus eliminating the additional injuries that would result to Plaintiff and Class.

158. Plaintiff and Class Members, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Sensitive Information not necessary for their provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory,

exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: June 13, 2023

THE SULTZER LAW GROUP P.C.

By: /s/ Jason P. Sultzer

Jason P. Sultzer, Esq.
Philip Furia, Esq.
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Tel: (845) 483-7100
Fax: (888) 749-7747
sultzerj@thesultzerlawgroup.com
furiap@thesultzerlawgroup.com

Counsel for Plaintiff and the Class

JS 44 (Rev. 4-29-21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MARK GUTHART on behalf of himself individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Nassau County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
The Sultzer Law Group P.C.
85 Civic Center Plaza, Ste. 200
Poughkeepsie, NY 12601
Jason P. Sultzer, Esq.
845-483-7100

DEFENDANTS

ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

Does this action include a motion for temporary restraining order or order to show cause? Yes ☐ No ☑"

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:

Brief description of cause:
Date Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 6/13/2023

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.7 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

Case is Eligible for Arbitration ☐

I, Jason P. Sultzer, counsel for Plaintiff and the Class, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☑ monetary damages sought are in excess of $150,000, exclusive of interest and costs,

☐ the complaint seeks injunctive relief,

☐ the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 1(c)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? ☐ Yes ☑ No

2.) If you answered "no" above:

a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? ☑ Yes ☐ No

b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? ☑ Yes ☐ No

c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received:

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? ☐ Yes ☐ No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

☑ Yes ☐ No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

☐ Yes (If yes, please explain ☑ No

I certify the accuracy of all information provided above.

Signature: _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

MARK GUTHART on behalf of himself individually and on behalf of all others similarly situated

Plaintiff(s)

v.

ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

Enzo Biochem, Inc.
81 Executive Blvd., Suite 3
Farmingdale, NY 11735

Enzo Clinical Labs, Inc.
28 Liberty Street
New York, NY 10005

Lab Corporation of America Holdings
531 South Spring Street
Burlington, NC 27215

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

The Sultzer Law Group P.C.
Jason P. Sultzer, Esq.
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

BRENNA B. MAHONEY
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: