UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MARIE V. NETROSIO, on behalf of herself and all others similarly situated, Plaintiff, v. **ENZO BIOCHEM, INC. AND ENZO CLINICAL LABS, INC.** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Marie Netrosio ("Plaintiff Netrosio"), individually and on behalf of all similarly situated persons, allege the following against Enzo Biochem, Inc. and Enzo Clinical Labs, Inc. (collectively, "Enzo" or "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Enzo for its failure to properly secure and safeguard Plaintiff's and other similarly situated Enzo patients' (or patients of Enzo's clients) personally identifiable information ("PII") and protected health information ("PHI"), including names, clinical test information, and Social Security numbers (the "Private Information"), from criminal hackers.

2. Enzo, which is based in Farmingdale, New York, is a life sciences and molecular diagnostics company that provides clinical research services and develops products such as DNA tests.

3. On or about May 30, 2023, Enzo filed documents with the Securities and Exchange Commission ("SEC") giving notice of "a ransomware attack that impacted certain information technology systems."[1] Under state and federal law, organizations must report breaches involving medical information within at least sixty (60) days.

4. On or about May 31, 2023, Enzo also sent out data breach letters to individuals whose Private Information was compromised as a result of the hacking incident.

5. Based on the notice Defendants filed with the SEC and the letter sent to Plaintiff Netrosio, Enzo's investigation revealed that an unauthorized party had access to certain files that contained sensitive information belonging to Plaintiff and Class Members, and that such access took place between April 4 and April 6, 2023 (the "Data Breach"). Although Defendants has stated that Social Security numbers of 600,000 of the 2,470,000 victims of the Data Breach "may have been involved," it has also stated that its investigation of the Data Breach "and the assessment of its impact is ongoing."[2]

6. In light of the highly sensitive information that was accessed and acquired as a result of the Data Breach, Plaintiff and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

[1] *See* https://www.sec.gov/Archives/edgar/data/316253/000121390023044007/ea178836-8k_enzobiohem.htm (last accessed June 11, 2023).
[2] *Id.*

7. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

8. There has been no assurance offered by Enzo that all personal data or copies of data have been recovered or destroyed, or that Defendants has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, lost value of their respective PII and PHI that was impacted in the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff brings this class action lawsuit to address Enzo's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Enzo, and thus Enzo was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, Enzo failed to properly monitor its systems and network that housed the Private Information and implement adequate data security practices with regard to such systems.

13. Plaintiff's and Class Members' identities are now at risk because of Enzo's negligent conduct as the Private Information that Enzo collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence per se, breach of third-party beneficiary contract, unjust enrichment/quasi contract, breach of confidence, and declaratory/injunctive relief.

II. PARTIES

16. Plaintiff Marie Netrosio is, and at all times mentioned herein was, an individual citizen of the State of New York.

17. Defendants Enzo Biochem, Inc. is incorporated in the State of New York, with its principal place of business at 81 Executive Blvd., Suite 3, Farmingdale, New York, Nassau County.

18. Enzo Clinical Labs, Inc. is incorporated in the State of New York, with its principal place of business at 60 Executive Boulevard, Farmingdale, New York, Nassau County.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Enzo. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Enzo because Enzo operates in and is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Enzo has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *Enzo's Business and Collection of Plaintiff's and Class Members' Private Information*

22. Enzo is a molecular diagnostics company, "leading the convergence of clinical laboratories, life sciences, and intellectual property through the development of unique diagnostic platform technologies that provide numerous advantages over previous standards."[3] Founded in 1976, Enzo is a global company located in the State of New York, serving millions of individuals through its three wholly-owned subsidiaries, Enzo Therapeutics, Enzo Life Sciences, and Enzo Clinical Labs, a named Defendant in this action.[4] Upon information and belief, Enzo employs over 400 individuals and generates over $100 million in annual revenue.

23. Enzo Clinical Labs is a full-service clinical reference laboratory, providing a "broad menu of routine and esoteric clinical assays utilizing the latest in laboratory technology[,] … assur[ing] a close working relationship between the laboratory and the medical professionals that [it] serve[s]."[5] This close working relationship "allows client physicians to request such items as personalized reporting protocols for abnormal results, and designing customized critical values."[6]

[3] *See* https://www.enzo.com/ (last visited on June 11, 2023)

[4] *Id*.

[5] *See* https://www.enzoclinicallabs.com/ (last visited on June 11, 2023).

[6] *Id*.

24. As a condition of receiving clinical services, Enzo requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Enzo, Plaintiff and Class Members were required to provide their Private Information to Defendants.

25. In its HIPAA Policy, Enzo states its understanding that "your medical information is private and confidential[,]" and that it is "required by law to maintain the privacy of 'protected health information.'"[7] Enzo also describes in its Privacy Policy the limited specific instances when it shares patient health information and says that it will otherwise share its patients' information "only with your permission in a written authorization."[8]

26. Defendants' joint HIPAA Policy defines "PHI" as "any individually identifiable information that we obtain from you or others that relates to your past, present or future physical or mental health, the health care you have received, or payment for your health care." Upon information and belief, Enzo obtained Plaintiff's Private Information from one of Plaintiff's medical providers – a client of Enzo's – and entered into an agreement with such client to safeguard and protect Plaintiff's Private Information in accordance with Defendants' HIPAA Policy.

27. Thus, due to the highly sensitive and personal nature of the information Enzo acquires and stores with respect to its patients, Enzo promises to, among other things: keep its patients' and its clients' patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients and its clients' patients of its legal duties relating to data security and comply with all federal and

[7] *See* https://www.enzoclinicallabs.com/footer-links/hipaa-policy (last visited on June 11, 2023).

[8] *Id.*

state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients and its clients' patients' if their Private Information is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Enzo assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. The Data Breach and Defendants' Inadequate Notice to Plaintiff and Class Members

29. According to Defendants' Notice, they learned of unauthorized access to their computer systems on April 6, 2023, with such unauthorized access having taken place between April 4 and April 6.

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including clinical treatment information and Social Security numbers. Defendants' investigation of the incident and the assessment of its impact is ongoing.

31. Enzo delivered the Notice to Plaintiff and Class Members on or around May 31, 2023, alerting them that their highly sensitive Private Information had been exposed in a ransomware attack. However, Enzo failed to offer any remedial assistance such as free credit monitoring, despite the serious nature of the attack and its ongoing investigation thereof.

32. Enzo had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to Enzo with the reasonable expectation and mutual understanding that Enzo would comply with its obligations to

keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. Enzo's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. Enzo knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

36. Enzo was on notice that companies in the healthcare industry are susceptible targets for data breaches.

37. Enzo was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[9]

38. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of

[9] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on June 11, 2023).

> patients' health and financial information, but also patient access to care.[10]

39. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[11] In 2022, the largest growth in compromises occurred in the healthcare sector.[12]

40. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13]

41. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[14]

---

[10] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on June 11, 2023).

[11] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on June 11, 2023).

[12] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on June 11, 2023).

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on June 11, 2023).

[14] *Id.*

42. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[15]

43. As a provider of clinical testing and other medical-related services, Enzo knew or should have known the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Enzo's patients as a result of a breach. Enzo failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Enzo Failed to Comply with HIPAA

44. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

45. Enzo's Data Breach resulted from a combination of insufficiencies that indicate Enzo failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Enzo's Data Breach that Enzo either failed to implement, or

[15] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on June 11, 2023).

inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

46. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

47. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

48. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

49. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

50. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

51. Based upon Defendants' Notice to Plaintiff and Class Members, Enzo reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

52. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

53. Enzo reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart

E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

54. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

56. Enzo reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

57. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

58. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

59. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

60. In addition, Enzo's Data Breach could have been prevented if Enzo had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

61. Enzo's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Enzo creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

62. Furthermore, Enzo is also a business associate under HIPAA.

63. HIPAA permits covered entities (such as the physician clients that provided Plaintiff's Private Information to Enzo) to disclose such information to business associates only if the covered entities obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.[16]

64. Upon information and belief, Enzo is a business associate as the type of functions and activities that fall within the purview of the Privacy Rule include, but are not limited to, claims processing or administration; data analysis; processing or administration; utilization review; quality assurance; benefit management; practice management; and repricing.

[16] *See* New HHS Fact Sheet On Direct Liability of Business Associates Under HIPAA, 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html (last visited on January 11, 2023).

65. In order to comply with the Privacy Rule, the satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.[17]

66. Thus, while it may not have made direct representations to Plaintiff regarding its data security and privacy obligations, practices and capabilities, Enzo is – further to HIPAA and its business associate agreement (the "BAA") requirements under the Privacy Rule – required to have a contract in place with each of its healthcare provider (covered entity) clients as a business associate under HIPAA, HITECH and any implementing regulations.

67. Thus, upon information and good faith belief, Enzo would have agreed to implement reasonable administrative, physical, technical and electronic safeguards to protect the confidentiality, integrity and availability of all Private Information provided to it by its clients.

68. Plaintiff and Class Members are intended third-party beneficiaries of any BAA between Enzo and its various healthcare/physician clients who are covered under HIPAA.

69. Because Enzo has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Enzo's approach to information security is adequate and appropriate going forward. Enzo still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. Enzo Failed to Comply with FTC Guidelines

70. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[17] *See* Business Associates, 45 CFR 164.502(e), 164.504(e), 164.532(d) & (e), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited on June 11, 2023).

According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

71. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

72. The FTC further recommends that companies not maintain PII 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. As evidenced by the Data Breach, Enzo failed to properly implement basic data security practices. Enzo's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

75. Enzo was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendants was also aware of the significant repercussions that would result from its failure to do so.

F. Enzo Failed to Comply with Industry Standards

76. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

77. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Enzo include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

78. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training

staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

79. 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.

80. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Enzo Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

81. In addition to its obligations under federal and state laws, Enzo owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Enzo owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

82. Enzo breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Enzo's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of patient Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

83. Enzo negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

84. Had Enzo remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

85. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Enzo.

H. Enzo Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

86. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[18] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

87. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

88. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[18] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on June 11, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

89. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

90. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts, insurance accounts, and/or financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

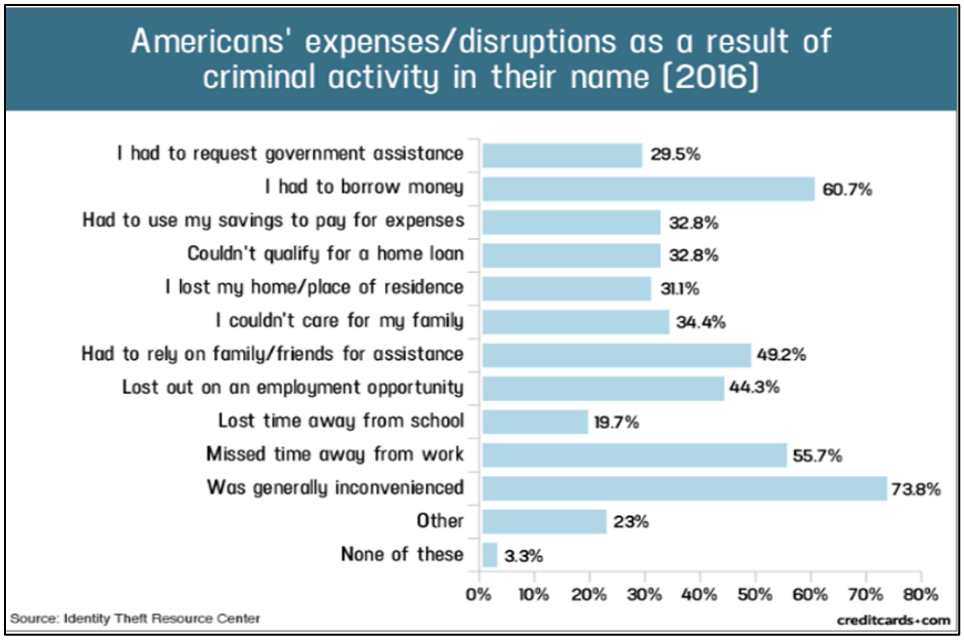
91. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[19] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

92. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the

[19] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited June 11, 2023).

thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

93. In fact, a study by the Identity Theft Resource Center[20] shows the multitude of harms caused by fraudulent use of PII:



94. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[21]

95. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[20] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on June 11, 2023).

[21] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on June 11, 2023).

96. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[22]

97. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

98. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[23]

99. The ramifications of Enzo's failure to keep its patients' and its clients' patients' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

100. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[22] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on June 11, 2023).

[23] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on June 11, 2023).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[24]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

101. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

102. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiff's and Class Members' Damages

Plaintiff Netrosio's Experience

103. Plaintiff Netrosio is unaware of how and when Enzo came into possession and control of her Private Information, though it is likely that Enzo is a business associate of one of Plaintiff Netrosio's medical providers.

104. On or about June 10, 2023, Plaintiff Netrosio received a letter informing her of the Data Breach, though the letter was vaguely worded and failed to offer any remedial or other assistance, despite the fact that Plaintiff is now at an increased risk of experiencing of identity theft, including but not limited to, potential medical fraud.

[24] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited June 11, 2023).

105. Plaintiff Netrosio suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

106. Plaintiff Netrosio would not have allowed her PII and PHI to be turned over to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard patient personal and health information from theft, and that those systems were subject to a data breach.

107. Plaintiff Netrosio suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

108. Plaintiff Netrosio suffered actual injury in the form of damages to and diminution in the value of her personal and health information – a form of intangible property that Plaintiff Netrosio entrusted to Defendants for the purpose of receiving healthcare services from Defendants and which was compromised in, and as a result of, the Data Breach.

109. Plaintiff Netrosio suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

110. Plaintiff Netrosio has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendants, are protected and safeguarded from future breaches.

111. As a result of the Data Breach, Plaintiff Netrosio made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants. Plaintiff Netrosio has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

112. As a result of the Data Breach, Plaintiff Netrosio has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Netrosio is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

113. Plaintiff Netrosio also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Netrosio; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

114. As a result of the Data Breach, Plaintiff Netrosio anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

115. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

116. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

117. As a direct and proximate result of Enzo's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans

opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

118. Further, and as set forth above, as a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

119. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

120. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

121. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

122. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

roughly $200 billion.[25] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[26] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[27]

123. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

124. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Enzo, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

125. As a direct and proximate result of Enzo's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

---

[25] See Data Coup, https://datacoup.com/.
[26] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/ (last visited Jan. 16, 2023).
[27] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 16, 2023).

V. CLASS ACTION ALLEGATIONS

126. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

127. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class" and "Class Members"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Enzo provided notice to Plaintiff and other Class Members beginning on or around May 31, 2023.

128. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

129. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

130. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

131. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 2.5 million individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Enzo's records, Class Members' records, publication notice, self-identification, and other means.

132. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Enzo engaged in the conduct alleged herein;

b. Whether Enzo's conduct violated the FTCA and/or HIPAA;

c. When Enzo learned of the Data Breach;

d. Whether Enzo's response to the Data Breach was adequate;

e. Whether Enzo unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Enzo failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Enzo's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Enzo's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Enzo owed a duty to Class Members to safeguard their Private Information;

j. Whether Enzo breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Enzo had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Enzo breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Enzo knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Enzo's misconduct;

p. Whether Enzo's conduct was negligent;

q. Whether Enzo's conduct was *per se* negligent;

r. Whether Enzo was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

133. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Enzo. Plaintiff are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there

are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

134. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

135. Predominance. Enzo has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Enzo's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

136. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Enzo. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

137. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Enzo has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

138. Finally, all members of the proposed Class are readily ascertainable. Enzo has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Enzo.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

139. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

140. Enzo knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

141. Enzo knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Enzo was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

142. Enzo owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Enzo's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

143. Enzo's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

144. Enzo's duty also arose because Defendants was bound by industry standards to protect its patients' confidential Private Information.

145. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Enzo owed them a duty of care to not subject them to an unreasonable risk of harm.

146. Enzo, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Enzo's possession.

147. Enzo, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

148. Enzo, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

149. Enzo breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and

e. Failing to comply with the FTCA.

150. Enzo had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Enzo with their Private Information was predicated on the understanding that Enzo would take adequate security precautions. Moreover, only Enzo had the ability to protect its systems (and the Private Information that it stored on them) from attack.

151. Enzo's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and/or misused, as alleged herein.

152. As a result of Enzo's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

153. Enzo's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

154. As a result of Enzo's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

155. Enzo also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

156. As a direct and proximate result of Enzo's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

157. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

158. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

159. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Enzo to, *inter alia*, strengthen its data security systems and monitoring

procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

160. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

161. Pursuant to Section 5 of the FTCA, Enzo had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

162. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq.*, Enzo had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

163. Specifically, pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

164. Enzo breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

165. Specifically, Enzo breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

166. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Enzo's duty in this regard.

167. Enzo also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

168. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Enzo's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

169. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Enzo's failure to comply with both constitutes negligence *per se*.

170. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Enzo's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

171. As a direct and proximate result of Enzo's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

172. As a direct and proximate result of Enzo's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

173. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Enzo to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

174. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

175. Upon information and belief, Defendants entered into contracts to provide services to their physician clients – Plaintiff's and Class Members' respective medical providers – which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to them.

176. Upon information and belief, these contracts are virtually identical to the contracts entered into between Defendants and its other physician clients around the country and the world whose patients were also affected by the Data Breach.

177. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendants agreed to receive and protect through their services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

178. Enzo knew that if it were to breach these contracts with its clients, the clients' patients, including Plaintiff and the Class, would be harmed by, among other harms, fraudulent transactions.

179. Enzo breached its contracts with the medical providers affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

180. As foreseen, Plaintiff and the Class were harmed by Enzo's failure to use reasonable data security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information.

181. Additionally, Enzo, as a business associate under HIPAA, was required to have business associate agreements in place with its covered entity medical provider clients. The Privacy Rule permits covered entities to disclose the Private Information of their patients to business associates only if the covered entities obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

182. Enzo is a business associate as the type of functions and activities that fall within the purview of the Privacy Rule. In order to comply with the Privacy Rule, the satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

183. Thus, while it may not have made representations directly to Plaintiff regarding its data security and privacy obligations, practices and capabilities, Enzo is—further to HIPAA and its BAA requirements under the Privacy Rule—required to have a contract in place with each of

its healthcare provider (covered entity) clients as a business associate under HIPAA, HITECH and any implementing regulations.

184. Thus, upon information and good faith belief, Enzo would have agreed to implement reasonable administrative, physical, technical and electronic safeguards to protect the confidentiality, integrity and availability of all Private Information provided to it by its clients.

185. Plaintiff and the Class Members are intended third-party beneficiaries of any BAA between Enzo and its various healthcare clients who are covered entities under HIPAA.

186. Any BAAs that Enzo is required to have with its covered entity clients must all include the following information, according to HHS:

a. A description of the permitted and required PHI used by the business associate/subcontractor;

b. A representation that the business associate/subcontractor will not use or further disclose PHI other than as permitted or required by the contract or as required by law; and

c. A requirement that the business associate/subcontractor will use appropriate safeguards to prevent inappropriate PHI use or disclosure.

See 45 CFR 164.504(e).

187. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

188. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

189. This Count is pleaded in the alternative to Count III above.

190. Plaintiff and Class Members conferred a monetary benefit on Defendants by providing their Private Information to Defendants.

191. In exchange, Plaintiff and Class members should have received from Defendant data storage that was compliant with and maintained in accordance with Defendant's pre-existing duties to secure such information under federal law and industry standards and were entitled to have Defendant protect their Private Information with adequate security.

192. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiff's and Class Members' Private Information for business purposes.

193. Defendant failed to secure Plaintiff's and Class Members' Private Information and therefore, did not provide full compensation for the benefit the Plaintiff's and Class Members' Private Information provided.

194. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

195. If Plaintiff and Class Members had known that Defendants would not secure their Private Information using adequate security, they would not have provided their information to Defendant's physician clients.

196. Plaintiff and Class Members have no adequate remedy at law. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on them.

197. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received.

COUNT V
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

198. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

199. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Enzo and ultimately accessed and acquired in the Data Breach.

200. As a healthcare provider and business associate, Enzo has a special, fiduciary relationship with its patients and clients' patients, including Plaintiff and Class Members. Because of that special relationship, Enzo was provided with and stored Plaintiff's and Class Members' Private Information and had a duty to maintain such Information in confidence.

201. Patients like Plaintiff and Class Members have a privacy interest in personal medical and other matters, and Enzo had a duty not to disclose such matters.

202. As a result of the parties' special relationship, Enzo had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiff and Class Members, information that was not generally known.

203. Plaintiff and Class Members did not consent nor authorize Defendants to release or disclose their Private Information to an unknown criminal actor.

204. Enzo breached its duty of confidence owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiff's and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards

in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

205. But for Enzo's wrongful breach of its duty of confidence owed to Plaintiff and Class Members, their Private Information would not have been compromised.

206. As a direct and proximate result of Enzo's wrongful breach of its duty of confidence, Plaintiff and Class Members have suffered and will continue to suffer the injuries alleged herein.

207. It would be inequitable for Enzo to retain the benefit of controlling and maintaining Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

208. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

209. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

210. 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 to grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

211. Enzo owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

212. Enzo still possesses Private Information regarding Plaintiff and Class Members.

213. Plaintiff alleges that Enzo's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

214. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Enzo owes a legal duty to secure its patients' Private Information and to timely notify customers of a data breach under the common law, HIPAA, and the FTCA;

b. Enzo's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. Enzo continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

215. This Court should also issue corresponding prospective injunctive relief requiring Enzo to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Enzo to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Enzo must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Enzo's systems on a periodic basis, and ordering Enzo to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Enzo's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Enzo's patients should take to protect themselves.

216. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Enzo. The risk of another such breach is real, immediate, and substantial. If another breach at Enzo occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

217. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Enzo if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Enzo's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Enzo has a pre-existing legal obligation to employ such measures.

218. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Enzo, thus preventing future injury to Plaintiff and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Enzo to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Enzo to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: June 12, 2023

Respectfully submitted,

/s/ Mason A. Barney

SIRI & GLIMSTAD LLP
Mason A. Barney
Tyler J. Bean (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

ClassAction.org