Letitia James
New York State Attorney General

Attorney General James Secures $4.5 Million from Biotech Company for Failing to Protect New Yorkers' Health Data

Data Breach of Lab Testing Company Enzo Exposed Health Information of Millions of Americans

August 13, 2024

NEW YORK – New York Attorney General Letitia James and the attorneys general of Connecticut and New Jersey today secured $4.5 million from Enzo Biochem, Inc. (Enzo) for failing to adequately safeguard the personal and private health information of its patients. Enzo is a biotechnology company that offers patients diagnostic testing at its laboratories in New York, Connecticut, and New Jersey. The Office of the Attorney General (OAG) found that Enzo had poor data security practices, which led to a ransomware attack that compromised the personal and private information of approximately 2.4 million patients, including more than 1.4 million New York residents. As a result of today's agreement, Enzo will pay $4.5 million, of which New York will receive $2.8 million, and will strengthen its data security practices.

"Getting blood work or medical testing should not result in patients having their personal and health information stolen by cybercriminals," said **Attorney General James**. "Health care companies like Enzo that do not prioritize data security put patients at serious risk of fraud and identity theft. Data security is part of patient safety, and my office will continue to hold companies accountable when they fail to protect New Yorkers."

In 2023, cyber-attackers were able to access Enzo's networks using two employee login credentials. The OAG later found that those two login credentials were shared between five Enzo employees and one of the login credentials hadn't been changed in the last ten years, putting Enzo at heightened risk of a cyberattack. Once logged in, the attackers installed malicious software on several of Enzo's systems. Enzo was not aware of the

attackers' activity until several days later because the company did not have a system or process in place to monitor or provide notice of suspicious activity. The attackers were able to steal files and data that contained patient information for 2.4 million patients, including 1,457,843 New Yorkers. Information that was compromised included names, addresses, dates of birth, phone numbers, Social Security numbers, and medical treatment/diagnosis information.

As a result of today's agreement, Enzo has agreed to pay a $4.5 million penalty, of which New York will receive $2.8 million, and adopt a series of measures aimed at strengthening its cybersecurity practices going forward, including:

- Maintaining a comprehensive information security program designed to protect the security, confidentiality, and integrity of private information;
- Implementing and maintaining policies and procedures that limit access to personal information;
- Implementing and maintaining multi-factor authentication for all individual user accounts;
- Establishing and maintaining policies and procedures that require using strong, complex passwords and password rotation;
- Encrypting all personal information, whether stored or transmitted;
- Conducting and documenting annual risk assessments; and
- Developing, implementing, and maintaining a comprehensive incident response plan for potential data security issues.

Attorney General James has taken several actions to hold companies accountable for having poor cybersecurity and to improve data security practices. Last month, Attorney General James launched two privacy guides, a Business Guide to Website Privacy Controls and a Consumer Guide to Tracking on the Web, to help businesses and consumers protect themselves. In July, Attorney General James issued a consumer alert to raise awareness about free credit monitoring and identity theft protection services available for millions of consumers impacted by the Change Healthcare data breach. In March 2024, Attorney General James led a bipartisan coalition of 41 attorneys general in sending a letter to Meta Platforms, Inc. (Meta) addressing the recent rise of Facebook and Instagram account takeovers by scammers and frauds. In April 2023, Attorney General James released a comprehensive data security guide to help companies strengthen their data security practices. In January 2022, Attorney General James

released a business guide for credential stuffing attacks that detailed how businesses could protect themselves and consumers.

This matter was handled by Senior Enforcement Counsel Jordan Adler and Deputy Bureau Chief Clark Russell of the Bureau of Internet and Technology, with special assistance from Internet and Technology Analyst Nishaant Goswamy, under the supervision of Bureau Chief Kim Berger. The Bureau of Internet and Technology is a part of the Division for Economic Justice, which is led by Chief Deputy Attorney General Chris D'Angelo and overseen by First Deputy Attorney General Jennifer Levy.