New York General Business Law (GBL)
Also known as the New York State Information Security Breach and Notification Act, this law was put into effect to ensure companies safeguard private information and notify individuals if a security breach could potentially put their private information at risk.

Elements of GBL §899-aa include:

- Security Breach Definition: The law defines a security breach as unauthorized access to or acquisition of, or access to or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.
- Personal Information Definition: Personal information under this law is described as any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.
- Private Information Definition: This is personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been accessed or acquired: Social Security number; driver's license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; biometric information; or username or email address in combination with a password or security question and answer that would permit access to an online account.
- Notification Requirement: If a business suffers a data breach, it is required to notify the individuals affected, the state attorney general, consumer reporting agencies, and other relevant parties.
- Penalties for Noncompliance: Non-compliant entities could face significant civil penalties for failing to adhere to the law.

Policy Reasons behind GBL §899-aa:

- Protecting Consumers: The primary motivation behind this law is to ensure the protection of consumers' private information. It aims to keep individuals informed about breaches that could impact their personal information.
- Promoting Transparency: The law also aims to promote transparency in how companies handle personal data, and in the event of a breach, making the affected individuals and the proper state authorities aware.
- Promoting Accountability: By imposing penalties for noncompliance, the law strives to make businesses more accountable for the security of personal information they hold.

New York General Business Law (GBL) §899-aa applies to all entities that store or process private information of New York residents, including non-profit organizations. Here's how this law might apply to a medium-sized non-profit organization accepting donations through their website:

- Collecting Personal Information: When accepting online donations, non-profits usually collect personal information such as names, addresses, and payment details. If any of this information is breached, it would fall under GBL §899-aa.
- Data Security Measures: Non-profits need to implement security measures to protect collected data. GBL §899-aa places a legal obligation on them to secure this private information.
- Notification Requirements: In the event of a data breach, the non-profit is required to promptly notify the affected individuals, the state attorney general, consumer reporting agencies, and other relevant parties.
- Penalties: If the non-profit fails to comply with these requirements, it could face significant civil penalties.
- Outsourced Data Management: If the non-profit uses third-party services for managing donations, it should ensure that these service providers are also compliant with GBL §899-aa.
- Implementation of Best Practices: While GBL §899-aa defines the bare minimum requirements, it is advisable for the non-profit to follow industry best practices for data security and breach notification, which might be even more stringent.

According to my training data, as of September 2021, the specific penalties for non-compliance with the New York General Business Law (GBL) §899-aa are as follows:

- Notification Failure: If a company, including a non-profit organization, fails to give notification in the manner required by law, they can be held liable for damages for actual costs or losses incurred by a person entitled to notice.
- Financial Penalties: A court can impose a civil penalty not exceeding $5,000 per violation. In the context of the law, a violation means a failure of notification to a single person. Therefore, if an organization fails to notify multiple people, the penalty would multiply accordingly.
- AG Enforcement: The attorney general may bring an action in his or her official capacity to address violations of this law and to impose penalties. This action would need to be commenced within two years of the date the attorney general became aware of the violation, or within two years of the date the violation should reasonably have been discovered with due diligence.
- Injunctive Relief: Along with or independent of the civil penalties, the court may also grant injunctive relief to prevent ongoing or future violations.

To ensure compliance with the New York General Business Law (GBL) §899-aa, a cybersecurity program for a medium non-profit educational organization can adopt several measures:

- Data Minimization: Collect only the necessary personal information required for donation and other operational purposes. The less data you have, the less there is to be compromised in a breach.
- Secure Data Storage and Transmission: Encrypt personal data at rest and in transit. This is a crucial step in protecting sensitive information from unauthorized access.

- Regular Security Audits: Conduct regular audits of security measures and data handling procedures to ensure compliance with the law and identify any potential vulnerabilities.
- Access Control: Implement strong access control policies. Only allow access to sensitive data to authorized personnel and ensure strong authentication mechanisms are in place.
- Security Awareness Training: Provide regular training to staff members about data security best practices, the importance of protecting personal information, and their roles in ensuring compliance with GBL §899-aa.

Reference:

New York State Legislature. (n.d.). GBS §899-aa: Disclosure; notification of breach of security of system. New York State Legislature. Retrieved from https://www.nysenate.gov/legislation/laws/GBS/899-AA