2022 GLBA Amendments

How to prepare for the biggest cybersecurity regulation change in two decades

MARCH 21 2022

GlobalCerts, LLC
Neil S. Gerard CISSP

Gramm Leach Bliley Act Safeguards Rule

A major facelift is coming to the 20 year old law

What is the Gramm Leach Bliley Act?

Congress enacted the Gramm Leach Bliley Act ("GLB" or "GLBA") in 1999. The Act is intended to provide strong privacy and security requirements for all financial institutions, with the ultimate goal of protecting the customers and their data. The act required the Federal Trade Commission to promulgate new laws regarding safeguarding customer data. They did so in 2002 with the 'Safeguards Rule' (16 CFR part 314). This regulation has been the driver of information security policy at most financial institutions for the last 20 years. This new amendment (Final Rule) brings major changes to this regulation.

Scope of the GLBA

The GLBA applies to all U.S. financial institutions. This certainly includes banks, credit unions, etc. But it also includes all types of organizations that handle the personal financial information of their customers. This includes pawnbrokers, educational institutions, accounting and bookkeeping firms, CPAs, etc.

With the new Final Rule, the GLBA further expands the scope to any entities the Federal Reserve Board finds are "incidental to financial activities". This includes banking intermediaries (a.k.a. 'finders') that connect prospective customers with financial institutions and brokers.

The FTC has also confirmed the type of information that is covered by the GLBA. It has doubled down that *customer information* is ANY information "containing nonpublic personal information". This can include things like the customer's full address or phone number, or even the fact that they have a bank account with a particular institution.

The Amendment

The GLBA amendment was issued as a *Final Rule* by the Federal Trade Commission (FTC) on December 9th, 2021. It has an "effective date" of January 10, 2022. However, the new provisions in part 314.5 will not be applicable until December 9th, 2022, 12 months after the final rule was issued.

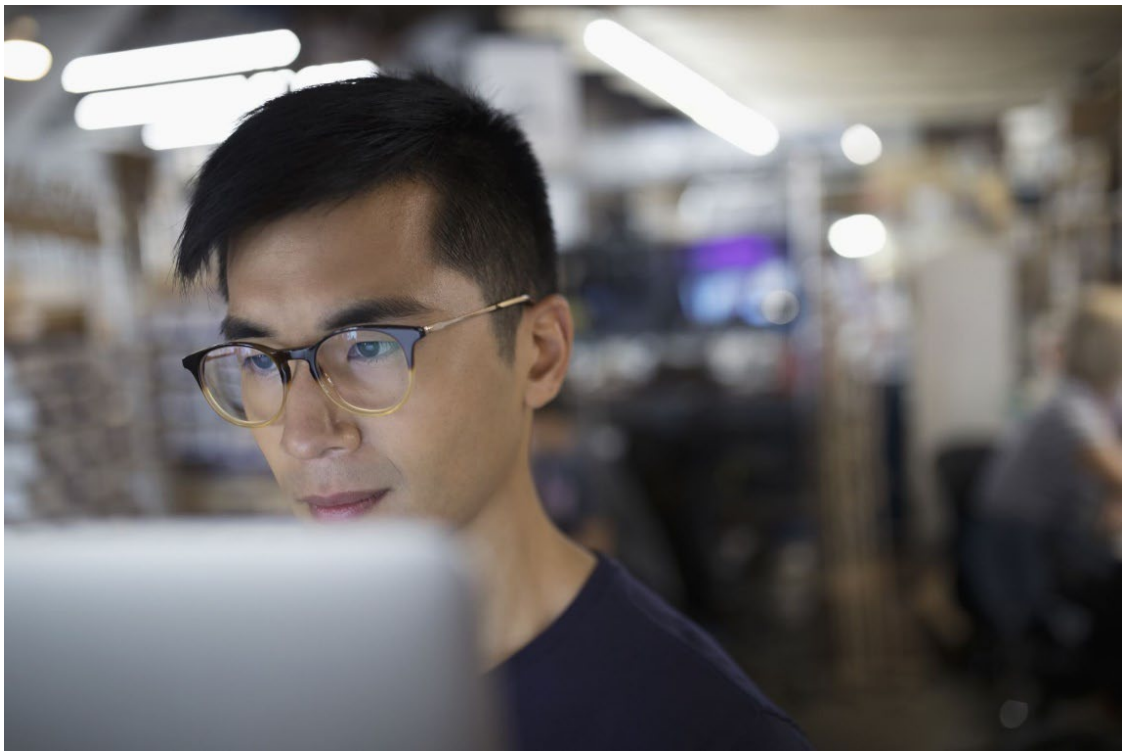
In essence, the rule puts a lot of "meat on the bones" of the original safeguards rule. It lays out much more specific security practices that covered organizations must follow. These include specific technical security controls like access control requirements, mandatory multi-factor authentication (MFA), encryption of data-at-rest and in-transit, etc. The rule also mandates things like requiring formal risk assessments, annual penetration tests, and semi-annual vulnerability assessments. It requires specific policies and practices for incident response, data retention, secure software development, change management, vendor risk management, and security awareness training. Overall, the new rule brings the GLBA in line with much more stringent security frameworks such as PCI-DSS and even NIST standards such as SP 800-171.

Main Criticisms

There has been a lot of industry push-back against the new requirements set forth by the FTC. One of the most common opinions among industry representatives was the high costs needed to implement all these requirements would drive smaller financial institutions out of business.

The FTC's counter-argument is that many of the requirements were already in place with the existing GLBA text requiring an information security program. They also indicate that there are free vulnerability scanners available and 'virtual CISO' services available to provide part-time help. They also argue that many applications and systems now have built-in encryption capabilities and that MFA can be acquired at low or no cost now, even by small businesses.

Breakdown of Major Changes



314.4 (a) Designation of a “Qualified Individual”

The GLBA already had a requirement to appoint an “employee or employees” to oversee and coordinate the information security program. This change requires that a *single* individual be identified, and ultimately responsible for the program. It does **not** mention any specific certifications or education required, so this could be the owner, head of IT, etc. The qualifications of the individual must simply be appropriate to the size/complexity of the organization.

314.4 (b)(1) Written Risk Assessment

The new GLBA Final Rule now requires financial institutions to maintain a formal risk management program including a written risk assessment as the main artifact. This is not a huge change from the previous law, as it already required the information security program to take a risk-based approach when establishing security policy and specific controls. The only difference is that it now requires the assessment to be a formal, written one with specific requirements, most likely requiring an information security professional’s assistance.

There are 3 required components of the risk assessment:

(i) Criteria for the evaluation and categorization of identified security risks or threats the financial institution faces;

This requires at least a basic qualitative ranking of identified risks (e.g. low, medium, high, critical) with a clear definition of criteria for each level.

(ii) criteria for the assessment of the confidentiality, integrity, and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats to the financial institution; and

Here, the organization is required to examine existing controls and determine to what degree they mitigate the identified risks. This is also known as a controls 'gap analysis'.

(iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the financial institution's risks.

For each identified risk, the organization will need to decide if existing controls are adequate, if additional controls must be implemented, or if the risk can be accepted. Risk acceptance can be a valid decision if the costs to mitigate the risks are higher than the potential costs if the risk is realized. However, this decision must be documented and approved by the Qualified Individual.

Also, note that there is no requirement for when risk assessments must be re-evaluated or updated, although best practice requires they be updated whenever the organization's assets, operations, or the threat landscape changes significantly.

This section does not apply to organizations holding information on fewer than 5,000 customers.

314.4 (c) Specific Required Security Controls

(1) Access Controls

This part requires access controls to be implemented on all information systems containing customer data, or to the information itself (in case of physical access to records). This provision also requires the 'principle of least privilege' to be applied by restricting the amount of customer data accessible to an employee to only what is required to perform their duties.

(2) System Inventory

Good asset management is vital to a well-run, efficient information security program. Knowing exactly what is in your environment and where data resides is the first step to securing it. The new rule requires organizations to identify all "data, personnel, devices, systems, and facilities" even if they do not handle customer information. This may be a completely new activity for many smaller organizations, but it is a necessary one.

(3) Encryption

This new section requires that organizations encrypt ALL customer information in transit and at rest, **or** adopt compensating controls approved by the Qualified

Individual. Note that this requirement does NOT apply to communications within the internal network of the organization, such as file sharing via SMB.

The biggest impacts this will have on many smaller organizations include (1) desktop/laptop systems may need to upgrade from Windows Home version to the Professional versions, which includes the built-in BitLocker encryption capabilities; and (2), if organizations use smartphones to access any client information, the devices must be encrypted and PIN-protected. This is a free and easy-to-use feature of all modern Android and Apple smartphones.

(4) Secure Software Development

This section mandates that any software developed in-house relating to customer information be done using secure development practices. This is a very vague requirement, but in general, this means the code has undergone static code analysis to look for common vulnerabilities and potentials for bugs like buffer overflows. There are open-source tools available like SonarQube that can perform such scans.

More crucially, the section also requires organizations to evaluate, assess, and test the security of any third-party software used with customer data. This could potentially be very onerous depending on the testing information available from the vendor. For web applications, organizations can leverage openly available tools such as OWASP ZAP that will look for common vulnerabilities like cross-site scripting, cross-site request forgery, SQL, and command injection.

(5) Multi-Factor Authentication

This section requires that access to any information systems that allow access to customer information MUST be protected by multi-factor authentication (MFA). Importantly, it does not prescribe the specific factors that can be utilized in authenticating access attempts. Organizations may use a variety of factors depending on the sensitivity of the data being protected (e.g. simple SMS verification for most systems, but perhaps a hardware token for the most sensitive systems).

This applies to access controls for all information systems, even to internal networks (local workstations). However, the rule does allow for “reasonably equivalent” controls subject to the written approval of the Qualified Individual.

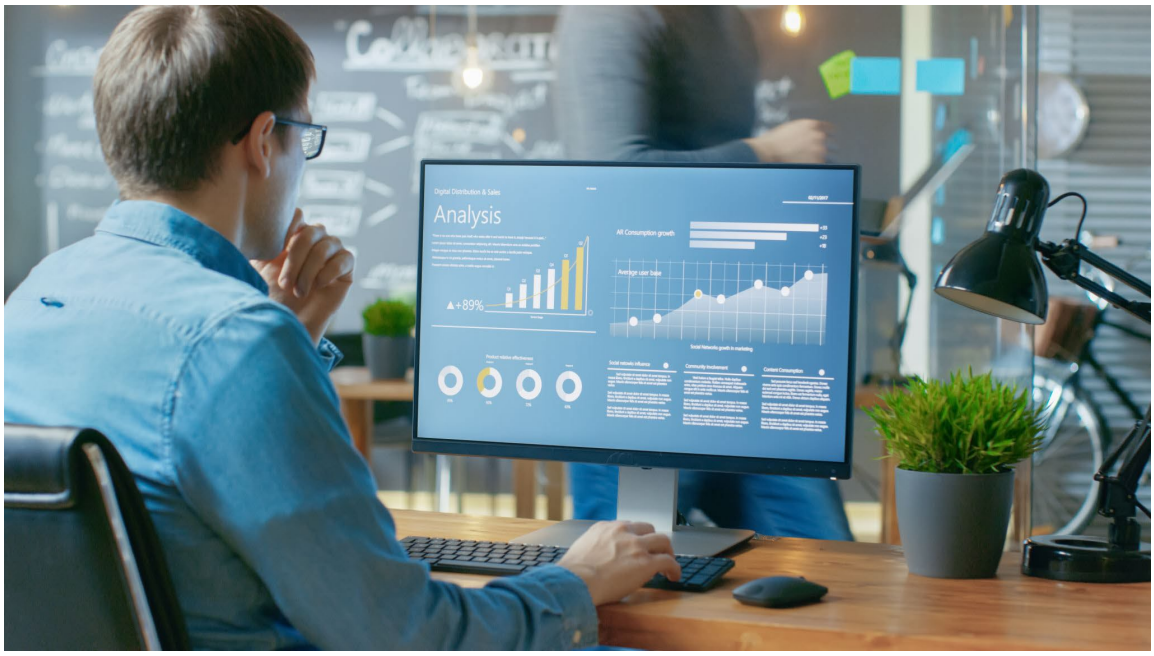
(6) Data Retention (Disposal)

Composed of 2 sections, the amendment will require organizations to securely dispose of customer information when it no longer serves a legitimate business use or 2 years after the information was last used to provide a product or service. For instance, if a customer applies for a loan or account, this application must be deleted after 2 years of processing. The second section also requires a periodic review of the organization's policies regarding data retention and disposal, with no hard time requirement.

This change may have a huge effect on accounting firms and CPAs. Archived tax returns are preserved based on complex IRS requirements that change depending on the type and attributes of the return. As a result, many firms choose to maintain archives for longer than required for uniformity. Now, this practice will potentially go against the section, and may also inadvertently put a firm over the 5,000 customer limit to qualify for the rule exceptions.

(7) Change Management

Organizations must adopt change management procedures to manage any changes within their information systems. This procedure must examine the security impact of any additions, removals, or changes in configurations to their information systems. It's important to recognize that change management procedures should be tailored to the size and complexity of the organization's IT infrastructure. As such, smaller organizations may only require a very basic change management policy where a checklist of security impacts is examined by the Qualified Individual and approved before the change is made.



(8) System Monitoring

The text of this section requires organizations “to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.” The key to this provision revolves around making sure that authenticated users are only accessing and modifying the customer information to which they are authorized. Note that this does NOT require a dedicated role to actively monitor data and system access. Several automated tools can provide such monitoring and notify one or more individuals that can take actions as a result.

It’s also important to note this requirement applies to paper records as well. This may require that access logs are kept when employees access customer file folders. Or, key cards could be used to automatically track access to storerooms, etc.

314.4 (D) (2) Penetration Testing and Vulnerability Scanning

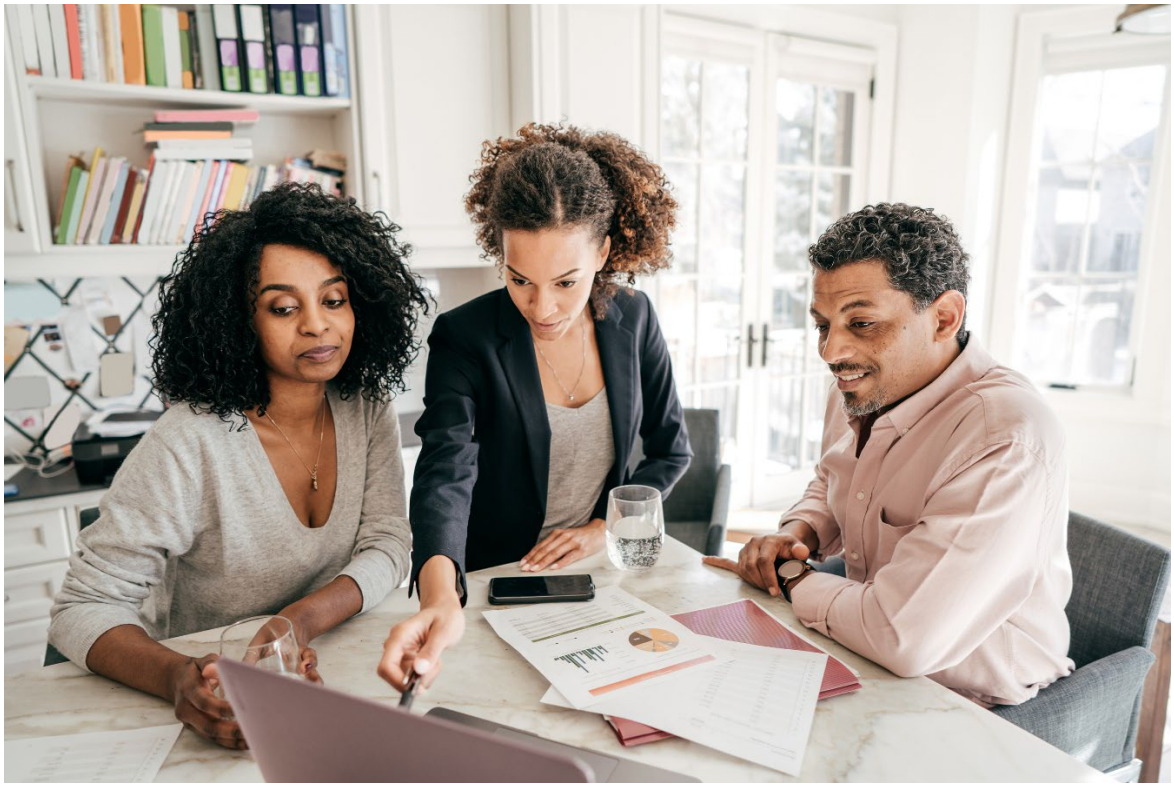
This paragraph is intended as a supplement to (d)(1), which requires regular testing and monitoring of safeguards, systems, and procedures to detect actual and attempted intrusions. The new paragraph goes much further in requiring either (1) continuous system monitoring, or (2) conducting a penetration test at least annually and a vulnerability scan at least semi-annually. It also requires

performing *additional* scans any time there are material changes in operations or assets.

Initially, this seems like a tremendous burden. However, this paragraph applies only to information systems (not physical infrastructure or controls) that are involved in processing, transmitting, or storing customer information. Correspondingly, the *scope* of any penetration tests and scans can be limited to a subset of the organization's IT systems, reducing costs.

This section does not apply to organizations holding information on fewer than 5,000 customers.

314.4 (E) Security Training



(1) Employee Training

This section requires that employees are specifically trained with materials that "reflect the risks identified in the risk assessment". For most smaller institutions, this requirement can be satisfied with general **"Security Awareness Training"** (SAT) available from several providers. Since smaller organizations aren't required to perform formal risk assessments, this requirement is

somewhat tempered. For larger organizations, they will be required to customize their SAT curriculum to reflect specific, identified risks.

(2) and (3) Information Security Personnel Training

The organization must use "qualified information security personnel" to manage organizational risk and the information security program. This paragraph specifically omits a specific description of the qualifications required by such personnel since it can wildly vary depending on the complexity of the organization's IT infrastructure. It also requires that organizations provide such personnel with "security updates and training sufficient to address relevant security risks." So, information security (IS) personnel must receive specific training above and beyond the SAT of regular employees.

Importantly, this section does not require any full-time employees to be dedicated to this role. Any combination of part-time work by existing staff or outsourced professionals can meet the requirement. From a cost reduction perspective, this would allow for smaller organizations to outsource both the creation and management of their information security program to a third-party contractor who specializes in IS risk management and IS governance. It is also assumed that these contractors will have received security updates and ongoing training as part of their profession.

(4) Continuing Education of Information Security

Information security threats and mitigation techniques are constantly changing in the cat-and-mouse game of cybersecurity. Consequently, it's crucial that the information security personnel within an organization continually update their knowledge on emerging threats and new security technologies. This requirement mandates that covered organizations will verify that IS personnel "take steps to maintain current knowledge of changing information security threats and countermeasures."

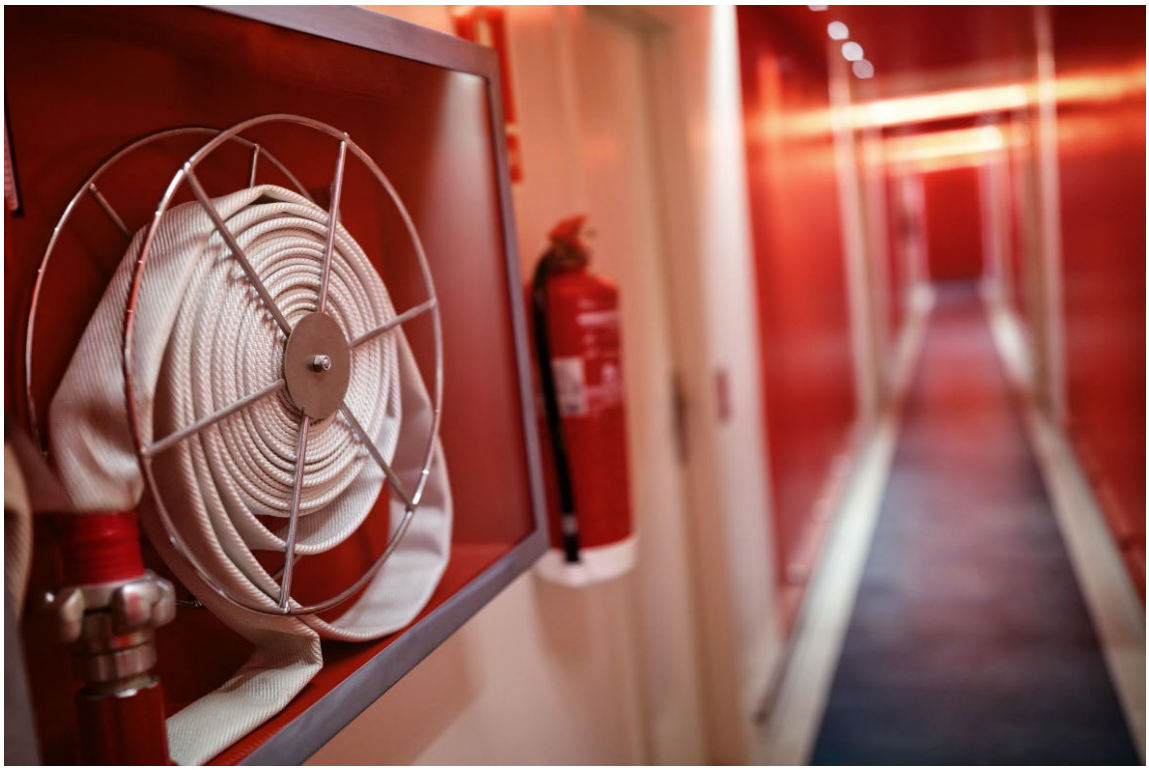
314.4 (F) Service Providers

(3) Vendor Risk Management

Organizations must periodically assess the risk presented by using 3rd party service providers. In essence, this rule requires organizations to ensure the

cloud services and other providers they are using have adequate security controls in place, and periodically check to make sure that's still the case. There aren't specific requirements for how this assessment must be accomplished. Most organizations will use a variety of tools, such as verifying that cloud providers have been audited as compliant with standards such as ISO 27001 and 27002.

However, it's important to note that verifying a certification or audit may not be sufficient for this requirement. A risk-based approach depending on the type and amount of customer information handled by the third party will guide what level of assessment is suitable for a given vendor. The policy regarding vendor security assessment should be a part of the organization's overall information security policy.



314.4 (h) Incident Response Planning

Organizations will now be required to establish a written incident response (IR) plan addressing 7 specific topics. The IR plan must be "designed to promptly respond to, and recover from, any security event materially affecting . . . customer information in your control". The plan must include:

(1) the goals of the plan; (2) the internal processes for responding to a security event; (3) the definition of clear roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (6) documentation and reporting regarding security events and related incident response activities; and (7) the evaluation and revision as necessary of the incident response plan following a security event.

It's vital to note that the plan need only address customer information directly in control of the organization. If a breach of a 3rd party holding customer data occurs, it does not need to be addressed in the scope of the IR plan.

Another important note is the absence of incident reporting requirements. Such requirements are a large part of other safeguard laws such as the Health Insurance Portability and Accountability Act (HIPAA). This requirement is currently under review and may form the basis for a new amendment in the future, but is not part of this amendment.

This section does not apply to organizations holding information on fewer than 5,000 customers.

214.4 (I) Accountability and Reporting

Without accountability to organizational leaders, information security programs can become misaligned with the overall business goals and focus of the organizations. To that effect, the new amendment requires the Qualified Individual to report to the board of directors or other similar executive roles at least annually. They must report on the status of the information security program, any material matters affecting security, and any recommendations or changes that may be required in the program.

For smaller organizations, this may simply be an annual summary by the head of information technology to the CEO or board of directors. This may be something that is already occurring at least annually.

This section does not apply to organizations holding information on fewer than 5,000 customers.

Next Steps

The GLBA amendments have been published as a Final Rule by the FTC, and according to Section 314.5, the effective date is just 12 months from publication. The countdown to December 9th, 2022 is fast approaching. Financial institutions, accounting firms, tax preparers, even pawnbrokers should gain an understanding of these changes and start preparing as soon as possible. Even smaller organizations that are exempted from some of the more onerous requirements may still face major new requirements. But the end result will be much-needed growth in the maturity and depth of their information security programs.

GlobalCerts has been helping financial institutions comply with the GLBA Safeguards rule since it became effective in 2003. We specialize in assisting smaller organizations to meet or exceed information security requirements established by law, without breaking the budget. Whether you just need a refresh of your information security plan to meet the new requirements, or you are starting from scratch, don't do it alone.

Contact us today for a free information security consultation:

https://globalcerts.com/consulting-services

+1 (855) 614-2378

sales@globalcerts.net

References:

https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

https://www.reuters.com/legal/transactional/new-safeguards-rule-how-will-it-impact-financial-institutions-2021-12-09/?fbclid=IwAR2O2oOLRg9PW9w91UddrVTaDKbcVz7JgkS3-S1hrBDkKadGEVcCMJNNYhw