**FTC Safeguards Rule Compliance Checklist**

**(As of 03/01/2024)**

|  |
| --- |
| **PART 314 – STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION (Safeguards Rule)** |
| Part 314 applies to handling customer information by all financial institutions over which the Federal Trade Commission (FTC) has jurisdiction. It applies to all financial information for customers with whom the institution has a relationship, as well as customer financial information provided by other financial institutions.[[1]](#footnote-1) |

|  |  |  |
| --- | --- | --- |
| **§314.3 – Standards for Safeguarding Customer Information** | **Y/N** | **Notes** |
| 1. Develop, implement, and maintain a comprehensive, written information security program that includes all elements set forth in §314.4 below. The program may include numerous policies, procedures, and standards. |  |  |
| 1. The program should achieve the following objectives: 2. Ensure the security and confidentiality of customer information; |  |  |
| 1. Protect against any anticipated threats or hazards to the security or integrity of such information; and |  |  |
| 1. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. |  |  |

| **§314.4 – Elements** | **Y/N** | **Notes** |
| --- | --- | --- |
| 1. **Qualified Individual** – Designate a “Qualified Individual” responsible for overseeing and implementing the program who may be an employee, affiliate, or service provider. If an affiliate or service provider is used, then the institution shall: |  |  |
| 1. Retain responsibility for compliance; |  |  |
| 1. Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and |  |  |
| 1. Require the service provider or affiliate to maintain an information security program that complies with Part 314. |  |  |
| 1. **Risk Assessment** – The risk assessment should:  * Identifyreasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information; and |  |  |
| * Assess the sufficiency of any safeguards in place to control these risks. |  |  |
| 1. The risk assessment shall be written[[2]](#footnote-2) and include: |  |  |
| * 1. Criteria for the evaluation and categorization of identified security risks or threats the institution faces; |  |  |
| * 1. Criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls in the context of identified risks or threats the institution faces; and |  |  |
| * 1. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks. |  |  |
| 1. Additional risk assessments should be periodically performed to reevaluate identified risks and reassess the sufficiency of safeguards in place to control the risks. |  |  |
| 1. **Control Design and Implementation** – Design and implement safeguards to control risks identified through the risk assessment process. |  |  |
| 1. Implement and periodically review access controls to authenticate and permit access only to authorized users and limit authorized users’ access to only customer information needed to perform duties or, in the case of customers, to access their own information. |  |  |
| 1. Identify and manage the data, personnel devices, systems, and facilities needed to achieve business purposes. |  |  |
| 1. Encrypt all customer information in transit and at rest if feasible. If not, effective alternative compensating controls reviewed and approved by the Qualified Individual may be used. |  |  |
| 1. Adopt secure development practices for in-house developed applications, including procedures for testing the security of externally developed applications used to transmit, access, or store customer information. |  |  |
| 1. Implement multi-factor authentication for any individual accessing any information systems unless the Qualified Individual has approved the use of reasonably equivalent or more secure access controls in writing. |  |  |
| 1. Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used unless necessary for business purposes, required by law or regulation, or targeted disposal is not reasonably feasible. The data retention policy should be reviewed periodically to minimize unnecessary retention of data. |  |  |
| 1. Adopt procedures for change management. |  |  |
| 1. Implement policies, procedures, and controls designed to monitor and log authorized user activity and detect unauthorized access or use of customer information. |  |  |
| 1. **Key Control Testing** – 2. Regularly test or otherwise monitor key controls identified during the risk assessment process. |  |  |
| 1. Monitoring and testing for information systems should include continuous monitoring or periodic penetration testing and vulnerability assessments[[3]](#footnote-3). At a minimum, penetration tests should be performed annually. Vulnerability assessments should be performed at least every six months, when there are material changes to operations or business arrangements, and when there are circumstances known or believed to have a material impact on the information security program. |  |  |
| 1. **Training and Expertise** – Implement policies and procedures to ensure personnel are able to enact the information security program. |  |  |
| 1. Security awareness training should be provided for all personnel that is updated as necessary to reflect risks identified by the risk assessment. |  |  |
| 1. Qualified information security personnel should be employed by you or engaged via outsourcing from an affiliate or service provider to manage information security risks and to perform or oversee the information security program. |  |  |
| 1. Information security personnel should receive security updates and training. |  |  |
| 1. Key information security personnel should take steps to maintain current knowledge of changing information security threats and countermeasures. |  |  |
| 1. **Service Providers** – Oversee service providers by: 2. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information; |  |  |
| 1. Requiring service providers by contract to implement and maintain safeguards; and |  |  |
| 1. Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards. |  |  |
| 1. **Program Adjustments** – Evaluate and adjust the information security program for:  * Key control testing and monitoring results; |  |  |
| * Material changes to operations or business arrangements; |  |  |
| * Risk assessment results; and |  |  |
| * Any circumstance that may have a material impact on the program. |  |  |
| 1. **Incident Response Plan[[4]](#footnote-4)** – Establish a written incident response plan to respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information. The plan shall address: |  |  |
| 1. Goals of the incident response plan; |  |  |
| 1. Internal processes for responding to a security event; |  |  |
| 1. Definition of clear roles, responsibilities, and levels of decision-making authority; |  |  |
| 1. External and internal communications and information sharing; |  |  |
| 1. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; |  |  |
| 1. Documentation and reporting regarding security events and related incident response activities; and |  |  |
| 1. Evaluation and revision as necessary of the plan following a security event. |  |  |
| 1. **Board Reporting[[5]](#footnote-5)** – Qualified Individual should report in writing to the board or equivalent governing body, annually at a minimum, the following: |  |  |
| 1. Overall status of the information security program |  |  |
| * Compliance with Part 314; and |  |  |
| 1. Material matters related to the program, such as: |  |  |
| * Risk assessment; |  |  |
| * Risk management and control decisions; |  |  |
| * Service provider arrangements; |  |  |
| * Results of testing; |  |  |
| * Security events or violations and management’s responses thereto; and |  |  |
| * Recommendations for changes. |  |  |
| 1. **Notification Events –** Notification events involving the information of at least 500 consumers trigger the requirement to notify the Commissioner. |  |  |
| The notification to the Commissioner is made as soon as possible, but no later than 30 days after the discovery of the event. |  |  |
| The notice is submitted on the FTC's website. Confirm that the notice includes: |  |  |
| * Name and contact information of the reporting financial institution. |  |  |
| * Description of the types of information involved in the event. |  |  |
| * Date or date range of the event if possible to determine. |  |  |
| * Number of affected or potentially affected consumers. |  |  |
| * General description of the event. |  |  |
| * Disclosure if law enforcement has issued a written determination to impede a criminal investigation or cause damage to national security. |  |  |
| 1. **Business Continuity and Disaster Recovery** – Establish a written plan addressing business continuity and disaster recovery. |  |  |

|  |  |  |
| --- | --- | --- |
| **§314.6 – Exceptions** | **Y/N** | **Notes** |
| Does the entity maintain customer information concerning fewer than five thousand consumers?  If yes, the following exceptions apply:   * §314.4(b)(1) – A **risk assessment** is required but is not required to be in writing. * §314.4(d)(2) – **Continuous monitoring, penetration testing, and vulnerability assessments** are not required; however, the institution must still regularly test or otherwise monitor the effectiveness of the information security program. * §314.4(h) – A written **Incident Response Plan** is not required. * §314.4(i) – **Annual written board reporting** is not required. |  |  |

1. Definitions of consumer and customer, among others, can be found in §314.2 [↑](#footnote-ref-1)
2. The risk assessment does not need to be in writing for financial institutions that maintain customer information concerning fewer than 5,000 consumers. However, a risk assessment does still need to be performed. [↑](#footnote-ref-2)
3. Continuous monitoring, penetration testing, or vulnerability assessments are not required for financial institutions that maintain customer information concerning fewer than 5,000 consumers. However, the effectiveness of the information security program must be regularly tested or otherwise monitored. [↑](#footnote-ref-3)
4. A written Incident Response Plan is not required for financial institutions that maintain customer information concerning fewer than 5,000 consumers. [↑](#footnote-ref-4)
5. Annual written board reporting is not required for financial institutions that maintain customer information concerning fewer than 5,000 consumers. [↑](#footnote-ref-5)