**CSBS MODEL NONBANK DATA SECURITY GUIDANCE**

State financial regulators are increasingly concerned with information security threats to U.S. financial systems. Cybercriminals can cause significant financial losses for institutions and consumers whose information may be revealed and/or stolen for illicit purposes. This guidance is intended as a basis for establishing a minimum set of information security safeguards and sets forth the supervisory expectation that you will assess and design a program that addresses your risk profile. It is imperative that senior management take this issue seriously and be responsible for the organization’s safeguards program.

This guidance applies to the handling of customer information by [IDENTIFY COVERAGE HERE], and applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a relationship or pertains to the customers of other institutions that have provided information to you. In general, the terms used in this guidance have the same meaning as set forth in the Federal Trade Commission’s Safeguards Rule[[1]](#footnote-1), which can be found here: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314>.

**Standards for Safeguarding Customer Information**

You should develop, implement, and maintain a comprehensive, written Information Security Program that contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any Customer Information at issue. Your Information Security Program should be designed to achieve the following objectives:

1. Ensure the security and confidentiality of Customer Information;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
4. Establish a written incident response plan and address business continuity and disaster recovery.

**Elements of an Effective Information Security Program**

* Qualified Individual: You should designate a qualified individual responsible for overseeing and enforcing your Information Security Program. This Qualified Individual may be employed by you, be an affiliate, or a contracted service provider. You should require your qualified individual to report in writing, at least annually, to your board of directors or senior management, the overall status of your information security program and your compliance with this Guidance and any applicable information security laws or rules.
* Information Security Oversight and Training: Implement policies and procedures to ensure that personnel are able to enact your Information Security Program by providing your personnel with security awareness training that is updated to reflect risks identified by the risk assessment.
* Risk Assessment: Base your Information Security Program on a risk assessment that identifies reasonably 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 assesses the sufficiency of any safeguards in place to control these risks. You should

periodically reassess your risks and the sufficiency of any safeguards in place or that are needed to address these risks.

* Safeguards: To control the risks you identify you should design and implement the appropriate safeguards including (this list is not exhaustive):
* *Access Controls* to authenticate and permit access only to authorized individuals

and restrict access at physical locations containing Customer Information.

* *Encryption* of all Customer Information held or transmitted by you.
* *Multi-factor Authentication* should be implemented for any individual accessing Customer Information, unless your qualified individual has approved the use of reasonably equivalent or more secure controls.
* *Secure Disposal of Customer Information:* Develop, implement, and maintain procedures for the secure disposal of Customer Information in any format that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
* Third Party Service Providers: If you use the services of a third party you should take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue and periodically assess their risk and the continued adequacy of their safeguards.
* Incident Response Plan: Establish a written incident response plan designed to promptly respond to, and recover from, any Security Event materially affecting the confidentiality, integrity, or availability of customer information in your possession. Such incident response plan should address the following areas:
1. Your internal processes for responding to a security event;
2. Identification of clear roles, responsibilities and levels of decision-making authority;
3. External and internal communications and information sharing;
4. Identification of requirements for the remediation of any identified weaknesses in your systems and associated controls;
5. Documentation and reporting regarding security events and related incident response activities; and
6. The evaluation and revision of the incident response plan following a security event.
* Notification Events: A notification event is the acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. You should notify the [Commissioner/Appropriate Contact] as promptly as possible following a security event, by contacting [Contact Information Here].

The following recommendations are intended for larger, more complex entities, or entities relying heavily on technology, whose security profiles dictate more sophisticated or robust controls:

* **Audit Trails:** Include audit trails within your information security program designed to detect and respond to security events.
* **Practices for In-House Developed Applications:** Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.
* **Change Management:** Adopt procedures for change management to document, track, test, approve and perform system and environmental changes.
* **Policies for Authorized Users:** Implement policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.
* **Penetration Testing and Vulnerability Assessments:** Regularly test or otherwise monitor the effectiveness of your safeguards’ key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into your systems. Your monitoring and testing should include continuous monitoring or periodic penetration testing and vulnerability assessments where feasible. If continuous monitoring is not feasible, you should conduct annual penetration testing and/or biannual vulnerability assessments.
1. Note the FTC’s Safeguards Rule includes several definitions and related examples, including the definition of “financial institution,” itself rather than incorporating them from another related FTC Rule, the Privacy of Consumer Financial Information Rule. This is done in an effort to make the rule more self-contained and to enable readers to understand its requirements without referencing the FTC’s Privacy of Consumer Financial Information Rule. [↑](#footnote-ref-1)