**CSBS Nonbank Model Data Security Law**

**Section 1.** **Title**

This Act shall be known and may be cited as the "CSBS Nonbank Model Data Security Law.” [replace with appropriate title]

**Section 2. Purpose and Intent – Coverage – Scope – Consistency – Substantial Compliance**

(a) Purpose and intent. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the agency head of a Security Event.

(b) Coverage. Persons or entities covered by this law are defined as “Financial Institutions” in Section 3*.* More specifically, covered Financial Institutions, persons or entities include, but are not limited to, mortgage lenders, ‘‘pay day’’ lenders, finance companies, mortgage brokers, money services businesses, check cashers, collection agencies, credit counselors, [list all appropriate entities]. They are referred to in this Act as ‘‘You.’’ This Act applies to all Customer Information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other Financial Institutions that have provided such information to you.

(c) Scope. This Act applies to the handling of Customer Information by all [Financial Institutions over which the commissioner … Insert language as appropriate].

(d) Consistency with federal regulation. This model is developed to incorporate 16 CFR Part 314, Standards for Safeguarding Customer Information, as proposed April 4, 2019 by the Federal Trade Commission, to implement sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, setting forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Customer Information.

(e) Substantial compliance. A Financial Institution, as described in Section 3, that can demonstrate substantial compliance with 16 CFR 314, as determined by the commissioner, shall be presumed compliant with the provisions of this Act.

(f) [Optional] This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

**Section 3 Definitions**

(a) In general. Except as modified by this Act or unless the context otherwise requires, the terms used in this Act have the same meaning as set forth in the Federal Trade Commission’s rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) “Authorized User” means any employee, contractor, agent, or other person that participates in your business operations and is authorized to access and use any of your Information Systems and data.

(c) “Customer Information” means any record containing nonpublic personal information, as defined in 16 CFR 313.3(n), about a customer of a Financial Institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(d) “Encryption” means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(e)(1) “Financial Institution” means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a Financial Institution. [Or insert state specific definition of covered persons.]

(2) Financial Institution does not include: [Insert entity types here or include an exemption section.]

(f) “Information Security Program” means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Customer Information.

(g) “Information System” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/ process controls systems, telephone switching and private branch exchange systems, and environmental controls systems.

(h) “Multi-factor Authentication” means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

(2) Possession factors, such as a token; or

(3) Inherence factors, such as biometric characteristics.

(i) “Penetration Testing” means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside your Information Systems.

(j) “Security Event” means an event resulting in unauthorized access to, or disruption or misuse of, an Information System or information stored on such Information System.

(k) “Service Provider” means any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to a Financial Institution that is subject to this Act.

**Section 4 Standards for safeguarding Customer Information.**

(a) Information Security Program. You shall develop, implement, and maintain a comprehensive Information Security Program that is written in one or more readily accessible parts and 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. The Information Security Program shall include the elements set forth in Section 5 and shall be reasonably designed to achieve the objectives of this Act, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of this section are to:

(1) Ensure the security and confidentiality of Customer Information;

(2) Protect against any 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.

**Section 5 Elements.**

In order to develop, implement, and maintain your Information Security Program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your Information Security Program and enforcing your Information Security Program (for purposes of this Act, ‘‘Chief Information Security Officer’’ or ‘‘CISO’’). The CISO may be employed by you, an affiliate, or a Service Provider. To the extent this requirement is met using a Service Provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this Act;

(2) Designate a senior member of your personnel responsible for direction and oversight of the CISO; and

(3) Require the Service Provider or affiliate to maintain an Information Security Program that protects you in accordance with the requirements of this Act.

(b) 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.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your Information Systems and Customer Information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(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 risks.

(2) You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identity through risk assessment, including:

(1) Place access controls on Information Systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of Customer Information and to periodically review such access controls;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Restrict access at physical locations containing Customer Information only to authorized individuals;

(4) Protect by Encryption all Customer Information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that Encryption of Customer Information, either in transit over external networks or at rest, is infeasible, you may instead secure such Customer Information using effective alternative compensating controls reviewed and approved by your CISO;

(5) 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;

(6) Implement Multi-factor Authentication for any individual accessing Customer Information. Multi- factor authentication shall be utilized for any individual accessing your internal networks that contain Customer Information, unless your CISO has approved in writing the use of reasonably equivalent or more secure access controls;

(7) Include audit trails within the Information Security Program designed to detect and respond to Security Events;

(8) 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;

(9) Adopt procedures for change management; and

(10) 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.

(d)(1) Regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, Information Systems.

(2) The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in Information Systems that may create vulnerabilities, you shall conduct:

(i) Annual Penetration Testing of your Information Systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Biannual vulnerability assessments, including any systemic scans or reviews of Information Systems reasonably designed to identify publicly known security vulnerabilities in your Information Systems based on the risk assessment.

(e) Implement policies and procedures to ensure that personnel are able to enact your Information Security Program by:

(1) Providing your personnel with security awareness training that is updated to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or Service Provider sufficient to manage your information security risks and to perform or oversee the Information Security Program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) Oversee Service Providers, by:

(1) Taking reasonable steps to select and retain Service Providers that are capable of maintaining appropriate safeguards for the Customer Information at issue;

(2) Requiring your Service Providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your Service Providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your Information Security Program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your Information Security Program.

(h) 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 shall address the following areas:

(1) The goals of the incident response 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.

(i) Require your CISO to report in writing, at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your Information Security Program. The report shall include the following information:

(1) The overall status of the Information Security Program and your compliance with this Act and associated rules; and

(2) Material matters related to the Information Security Program, addressing issues 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 in the Information Security Program.

(j) Establish a written plan addressing business continuity and disaster recovery.

**Section 6 Effective date.**

Sections [XXXXXX] are effective as of [when].

**[Optional] Section 7 Exceptions.**

Sections [XXXXXX] do not apply to Financial Institutions that [e.g. maintain Customer Information concerning fewer than five thousand consumers; insert as appropriate].

**Section 8 Alteration of Federal Regulation**

If an alteration of Federal regulations under subsection 2(d) results in a complete lack of Federal regulations in the area:

(a) The version of the state requirements in effect at the time of the alteration shall remain in effect for [two years].

(b) During the time period under paragraph (a), the department shall promulgate replacement regulations as necessary and appropriate.

**[Optional] Section 9 Notification of a Security Event**

(a) Notification to the [Commissioner]**.** Each covered Financial Institution shall notify the [Commissioner] as promptly as possible but in no event later than 72 hours from a determination that a Security Event has occurred when the Financial Institution reasonably believes that the Customer Information involved is of 250 or more Consumers residing in this [state] and that is either of the following:

(1) A Security Event impacting the Financial Institution of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

(2) A Security Event that has a reasonable likelihood of materially harming:

(i) Any Consumer residing in this [state]; or

(ii) Any part of the normal operation(s) of the Financial Institution.

(3) The [Commissioner] shall promulgate rules detailing the format and requirements of notice.

(b) Notice Regarding Security Events of Service Providers

(1) In the case of a Security Event in a system maintained by a Service Provider, of which the Financial Institution has become aware, the Financial Institution shall treat such event as it would under subsection 9(a).

(2) The computation of the Financial Institution’s deadlines shall begin on the day after the Service Provider notifies the Financial Institution of the Security Event or the Financial Institution otherwise has actual knowledge of the Security Event, whichever is sooner.

**Section 10 Power of [Commissioner]**

(a) The [Commissioner] shall have power to examine and investigate into the affairs of any covered Financial Institution to determine whether the Financial Institution has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the [Commissioner] has under [include appropriate citation].

(b) Whenever the Commissioner has reason to believe that a Financial Institution has been or is engaged in conduct in this [state] that violates this Act, the [Commissioner] may take action that is necessary or appropriate to enforce the provisions of this Act.

**[Optional] Section 11. Public Disclosure and Confidentiality**

[Each state should consider appropriate disclosure and confidentiality requirements.]