CHAPTER 13-01.2
FINANCIAL INSTITUTION DATA SECURITY PROGRAM

13-01.2-01. Definitions.

For purposes of this chapter, the following definitions shall apply:

1. "Authorized user" means any employee, contractor, agent, or other person who:
   a. Participates in a financial corporation's business operations; and
   b. Is authorized to access and use any of the financial corporation's information systems and data.
2. "Commissioner" means the commissioner of the department of financial institutions.
3. "Consumer":
   a. Means an individual, or that individual's legal representative, who applies for or has obtained a financial product or service from a financial corporation which is to be used primarily for personal, family, or household purposes. A consumer includes an individual who:
      (1) Applies to a financial corporation for credit for personal, family, or household purposes, regardless of whether the credit is extended.
      (2) Provides nonpublic personal information to a financial corporation to obtain a determination about whether the applicant may qualify for a loan to be used primarily for personal, family, or household purposes, regardless of whether the loan is extended.
      (3) Provides nonpublic personal information to a financial corporation in connection with obtaining or seeking to obtain financial, investment, or economic advisory services, regardless of whether the financial corporation establishes a continuing advisory relationship.
      (4) Has a loan for personal, family, or household purposes in which the financial corporation has ownership or servicing rights, even if the financial corporation or one or more other corporations that hold ownership or servicing rights in conjunction with the financial corporation hires an agent to collect on the loan.
   b. Does not include an individual who:
      (1) Uses a different financial corporation or financial institution to act solely as an agent for, or provide processing or other services to, the individual financial corporation or financial institution.
      (2) Designates a financial corporation solely for the purposes to act as trustee for a trust.
      (3) Is a beneficiary of a trust for which the financial corporation is a trustee.
      (4) Is a participant or a beneficiary of an employee benefit plan that the financial corporation sponsors or for which the financial corporation acts as a trustee or fiduciary.
4. "Continuing relationship":
   a. Means a situation in which a consumer:
      (1) Has a credit or investment account with a financial corporation;
      (2) Obtains a loan from a financial corporation;
      (3) Purchases an insurance product from a financial corporation;
      (4) Holds an investment product through a financial corporation, including when a financial corporation acts as a custodian for securities or for assets in an individual retirement arrangement;
      (5) Enters into an agreement or understanding with a financial corporation in which the financial corporation undertakes to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;
      (6) Enters into a lease of personal property on a nonoperating basis with a financial corporation;
      (7) Obtains financial, investment, or economic advisory services from a financial corporation for a fee;

(8) Becomes a financial corporation's client for the purpose of obtaining tax preparation or credit counseling services from the financial corporation;
(9) Obtains career counseling while:
(a) Seeking employment with a financial corporation or the finance, accounting, or audit department of any company; or
(b) Employed by a financial corporation or department of any company;
(10) Is obligated on an account that a financial corporation purchases from another financial corporation, regardless of whether the account is in default when purchased, unless the financial corporation does not locate the consumer or attempt to collect any amount from the consumer on the account;
(11) Obtains real estate settlement services from a financial corporation; or
(12) Has a loan for which a financial corporation owns the servicing rights.

b. Does not include a situation in which:
(1) The consumer obtains a financial product or service from a financial corporation only in isolated transactions, including:
(a) A financial corporation's automated teller machine to withdraw cash from an account at another financial institution;
(b) Purchasing a money order from a financial corporation;
(c) Cashing a check with a financial corporation; or
(d) Making a wire transfer through a financial corporation;
(2) A financial corporation sells the consumer's loan and does not retain the rights to service that loan;
(3) A financial corporation sells the consumer an airline ticket, travel insurance, or a traveler's check in isolated transactions;
(4) The consumer obtains one-time personal or real property appraisal services from a financial corporation; or
(5) The consumer purchases checks for a personal checking account from a financial corporation.

5. "Customer" means a consumer who has a customer relationship with a financial corporation.
6. "Customer information" means any record containing nonpublic personal information about a customer of a financial corporation, whether in paper, electronic, or other form, which is handled or maintained by or on behalf of the financial corporation or the financial corporation's affiliates.
7. "Customer relationship" means a continuing relationship between a consumer and a financial corporation under which the financial corporation provides one or more financial products or services to the consumer that are used primarily for personal, family, or household purposes.
8. "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, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.
9. "Financial corporation" means all entities regulated by the department of financial institutions, excluding financial institutions and credit unions.
10. "Financial institution" means any bank, industrial loan company, or savings and loan association organized under the laws of this state or of the United States.
11. "Financial product or service" means any product or service that a financial holding company could offer by engaging in a financial activity under the federal Bank Holding Company Act of 1956 [12 U.S.C. 1843 section 4(k)]. The term includes a financial corporation's evaluation or brokerage of information that a financial corporation collects in connection with a request or an application from a consumer for a financial product or service.
12. "Information security program" means the administrative, technical, or physical safeguards a financial corporation uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

13. "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, including industrial process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contain customer information or that is connected to a system that contains customer information.
14. "Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors:
    a. Knowledge factors, including a password;
    b. Possession factors, including a token; or
    c. Inherence factors, including biometric characteristics.
15. "Nonpublic personal information":
    a. Means:
        (1) Personally identifiable financial information; and
        (2) Any list, description, or other grouping of consumers, including publicly available information pertaining to the consumers that is derived using personally identifiable financial information that is not publicly available, including account numbers.
    b. Does not include:
        (1) Publicly available information, except as included on a list described in paragraph 2 of subdivision a;
        (2) Any list, description, or other grouping of consumers, including publicly available information pertaining to the consumers that is derived without using any personally identifiable financial information that is not publicly available; or
        (3) Any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any individual on the list is the financial corporation's consumer.
16. "Notification event" means the acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered unencrypted for purposes of this subsection if the encryption key was accessed by an unauthorized person. Unauthorized acquisition is presumed to include unauthorized access to unencrypted customer information unless the financial corporation has reliable evidence showing there has not been, or could not reasonably have been, unauthorized acquisition of customer information.
17. "Penetration testing" means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting to penetrate databases or controls from outside or inside a financial corporation's information systems.
18. "Personally identifiable financial information":
    a. Means any information:
        (1) A consumer provides to a financial corporation to obtain a financial product or service;
        (2) About a consumer resulting from any transaction involving a financial product or service between a financial corporation and a consumer; or
        (3) A financial corporation otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.
    b. Includes:
        (1) Information a consumer provides to a financial corporation on an application to obtain a loan, credit card, or other financial product or service;
        (2) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
        (3) An individual that is or has been a financial corporation's customer or has obtained a financial product or service from the financial corporation;

(4) Any information about a financial corporation's consumer if it is disclosed in a manner that indicates the individual is or has been a financial corporation's consumer;
(5) Any information a consumer provides to a financial corporation or which a financial corporation or a financial corporation's agent otherwise obtains in connection with collecting on, or servicing, a credit account;
(6) Any information a financial corporation collects through an information collecting device from a web server; and
(7) Information from a consumer report.

c. Does not include:
(1) A list of names and addresses of customers of an entity that is not a financial corporation; and
(2) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

19. a. "Publicly available information":
(1) Means any information that a financial corporation has a reasonable basis to believe is lawfully made available to the general public from:
(a) Federal, state, or local government records;
(b) Widely distributed media; or
(c) Disclosures to the general public which are required under federal, state, or local law.
(2) Includes information:
(a) In government real estate records and security interest filings; or
(b) From widely distributed media, a telephone book, a television or radio program, a newspaper, or a website that is available to the general public on an unrestricted basis. A website is not restricted because an internet service provider or a site operator requires a fee or a password, provided access is available to the general public.

b. For purposes of this subsection, a financial corporation has a reasonable basis to believe information is lawfully made available to the general public if the financial corporation has taken steps to determine:
(1) The information is of the type available to the general public; and
(2) Whether an individual can direct that the information not be made available to the general public and, if so, that the financial corporation's consumer has not done so. A financial corporation has a reasonable basis to believe mortgage information is lawfully made available to the general public if the financial corporation determines the information is of the type included on the public record in the jurisdiction where the mortgage is recorded. A financial corporation has a reasonable basis to believe an individual's telephone number is lawfully made available to the general public if the financial corporation has located the telephone number in the telephone book or the consumer has informed the financial corporation the telephone number is not unlisted.

20. "Qualified individual" means the individual designated by a financial institution to oversee, implement, and enforce the financial institution's information security program.

21. "Security event" means an event resulting in unauthorized access to, or disruption or misuse of:
a. An information system or information stored on an information system; or
b. Customer information held in physical form.

22. "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 corporation that is subject to this chapter.

13-01.2-02. Standards for safeguarding customer information.

1. A financial corporation shall develop, implement, and maintain a comprehensive information security program.
2. The information security program must:
   a. Be written in one or more readily accessible parts; and
   b. Maintain administrative, technical, and physical safeguards that are appropriate to the financial corporation's size and complexity, the nature and scope of the financial corporation's activities, and the sensitivity of any customer information at issue.
3. The financial corporation shall develop a security program that:
   a. Ensures the security and confidentiality of customer information;
   b. Protects against any anticipated threats or hazards to the security or integrity of such information; and
   c. Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

13-01.2-03. Elements of a security program.

1. A financial corporation's information security program must denote a designation of a qualified individual responsible for overseeing and implementing the financial corporation's information security program and enforcing the financial corporation's information security program. The qualified individual may be employed by the financial corporation, an affiliate, or a service provider.
2. If a financial corporation designates an individual employed by an affiliate or service provider as the qualified individual, the financial corporation shall:
   a. Retain responsibility for compliance with this chapter;
   b. Designate a senior member of the financial corporation's personnel to be responsible for directing and overseeing the qualified individual; and
   c. Require the service provider or affiliate to maintain an information security program that protects the financial corporation in accordance with the requirements of this chapter.
3. A financial corporation shall base the financial corporation's information security program on a risk assessment that:
   a. 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 customer information;
   b. Assesses the sufficiency of any safeguards in place to control the risks in subdivision a; and
   c. Includes additional periodic risk assessments that:
      (1) Re-examine 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
      (2) Reassess the sufficiency of any safeguards in place to control these risks.
4. The risk assessment must be in writing and include:
   a. Criteria to evaluate and categorize identified security risks or threats the financial corporation faces;
   b. Criteria for the assessment of the confidentiality, integrity, and availability of the financial corporation's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats the financial corporation faces; and
   c. Requirements describing how:
      (1) Identified risks will be mitigated or accepted based on the risk assessment; and
      (2) The information security program will address the risks.

5. A financial corporation shall design and implement safeguards to control the risks the financial corporation identifies through the risk assessment in subsection 4, which include:
    a. Implementing and periodically reviewing access controls, including technical and as appropriate, physical controls to:
        (1) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and
        (2) Limit an authorized user's access to only customer information the authorized user needs to perform the authorized user's duties and functions, or in the case of a customer, to access the customer's own information.
    b. Identifying and managing data, personnel, devices, systems, and facilities that enable the financial corporation to achieve business purposes in accordance with the business purpose's relative importance to business objectives and the financial corporation's risk strategy.
    c. Protecting by encryption all customer information held or transmitted by the financial corporation both in transit over external networks and at rest. To the extent a financial corporation determines that encryption of customer information, either in transit over external networks or at rest, is infeasible, the financial corporation may secure customer information using effective alternative compensating controls reviewed and approved by the financial corporation's qualified individual.
    d. Adopting secure development practices for in-house developed applications utilized by the financial corporation for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications the financial corporation utilizes to transmit, access, or store customer information.
    e. Implementing multifactor authentication for any individual accessing any information system, unless the financial corporation's qualified individual has approved in writing the use of a reasonably equivalent or more secure access control.
    f. Developing, implementing, and maintaining procedures to securely dispose of customer information, in any format, no later than two years after the last date the information is used in connection with providing a product or service to the customer which it relates, unless:
        (1) The information is necessary for business operations or for other legitimate business purposes;
        (2) Is otherwise required to be retained by law or regulation; or
        (3) Where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
    g. Periodically reviewing the financial corporation's data retention policy to minimize unnecessary retention of data.
    h. Adopting procedures for change management.
    i. Implementing policies, procedures and controls designed to:
        (1) Monitor and log the activity of authorized users; and
        (2) Detect unauthorized access to, use of, or tampering with customer information by authorized users.
6. a. A financial corporation shall regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including the controls, systems, and procedures to detect actual and attempted attacks on, or intrusions into, information systems.
    b. Information systems monitoring and testing must include continuous monitoring or periodic penetration testing, and vulnerability assessments. Without effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, a financial corporation shall conduct:

(1) Annual penetration testing of the financial corporation's information systems based on relevant identified risks in accordance with the risk assessment; and
(2) Vulnerability assessments, including systemic scans or information systems reviews that are reasonably designed to identify publicly known security vulnerabilities in the financial corporation's information systems based on the risk assessment, at least every six months; whenever there are material changes to the financial corporation's operations or business arrangements; and whenever there are circumstances the financial corporation knows or has reason to know may have a material impact on the financial corporation's information security program.

7. A financial corporation shall implement policies and procedures to ensure the financial corporation's personnel are able to enact the financial corporation's information security program by:
   a. Providing the financial corporation's personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
   b. Utilizing qualified information security personnel employed by the financial corporation or an affiliate or service provider sufficient to manage the financial corporation's information security risks and to perform or oversee the information security program;
   c. Providing information security personnel with security updates and training sufficient to address relevant security risks; and
   d. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.
8. A financial corporation shall oversee service providers by:
   a. Taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information;
   b. Requiring, by contract, the financial corporation's service providers implement and maintain appropriate safeguards; and
   c. Periodically assessing the financial corporation's service providers based on the risk they present, and the continued adequacy of the service providers' safeguards.
9. A financial corporation shall evaluate and adjust the financial corporation's information security program by incorporating:
   a. The results of the testing and monitoring required under subsection 5;
   b. Any material changes to the financial corporation's operations or business arrangements;
   c. The results of risk assessments performed under subsection 3; or
   d. Any other circumstances that the financial corporation knows or has reason to know may have a material impact on the financial corporation's information security program.
10. A financial corporation shall 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 the financial corporation controls. The plan must address:
    a. The goals of the incident response plan;
    b. The internal processes for responding to a security event;
    c. Clear roles, responsibilities, and levels of decisionmaking authority;
    d. External and internal communications and information sharing;
    e. Requirements for the remediation of any identified weaknesses in information systems and associated controls;
    f. Documentation and reporting regarding security events and related incident response activities; and
    g. The evaluation and revision of the incident response plan, as necessary, after a security event.

11. A financial corporation shall require the financial corporation's qualified individual to report in writing, at least annually, to the financial corporation's board of directors or equivalent governing body. If no board of directors or equivalent governing body exists, the report shall be timely presented to a senior officer responsible for the financial corporation's information security program. The report must include:
    a. The overall status of the information security program, and the financial corporation's compliance with this chapter and associated rules; and
    b. Material matters related to the information security program, addressing issues including 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.
12. a. A financial corporation shall notify the commissioner about notification events.
    b. After discovery of a notification event described in subdivision c, if the notification event involves the information of at least five hundred consumers, the financial corporation shall notify the commissioner as soon as possible, and no later than forty-five days after the event is discovered. The notice must be made in a format specified by the commissioner and include:
        (1) The name and contact information of the reporting financial corporation;
        (2) A description of the types of information involved in the notification event;
        (3) The date or date range of the notification event, if the information is possible to determine;
        (4) The number of consumers affected or potentially affected by the notification event;
        (5) A general description of the notification event; and
        (6) A statement whether any law enforcement official has provided the financial corporation with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the commissioner to contact the law enforcement official. A law enforcement official may request an initial delay of up to forty-five days following the date when notice was provided to the commissioner. The delay may be extended for an additional period of up to sixty days if the law enforcement official seeks an extension in writing.
    c. A notification event must be treated as discovered on the first day when the event is known to the financial corporation. A financial corporation is deemed to have knowledge of a notification event if the event is known to any employee, officer, or other agent of the financial corporation, other than the person committing the breach.
13. A financial corporation shall establish a written plan addressing business continuity and disaster recovery.

13-01.2-04. Exemptions.

Subsection 4, subdivision b of subsection 6, and subsections 10 and 11 of section 13-01.2-03 do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.