Senator ..... moves to amend S.F. No. 4157 as follows:

Page 1, before line 11, insert:

"Section 1. **[46A.01] DEFINITIONS.**

Subdivision 1. **Terms.** For the purposes of this chapter, the terms defined in this section have the meanings given them.

Subd. 2. **Authorized user.** "Authorized user" means any employee, contractor, agent, or other person who: (1) participates in a financial institution's business operations; and (2) is authorized to access and use any of the financial institution's information systems and data.

Subd. 3. **Commissioner.** "Commissioner" means the commissioner of commerce.

Subd. 4. **Consumer.** (a) "Consumer" means an individual who obtains or has obtained from a financial institution a financial product or service that is used primarily for personal, family, or household purposes, or is used by the individual's legal representative. Consumer includes but is not limited to an individual who:

(1) applies to a financial institution for credit for personal, family, or household purposes, regardless of whether the credit is extended;

(2) provides nonpublic personal information to a financial institution in order to obtain a determination whether the individual qualifies for a loan used primarily for personal, family, or household purposes, regardless of whether the loan is extended;

(3) provides nonpublic personal information to a financial institution in connection with obtaining or seeking to obtain financial, investment, or economic advisory services, regardless of whether the financial institution establishes a continuing advisory relationship with the individual; or

(4) has a loan for personal, family, or household purposes in which the financial institution has ownership or servicing rights, even if the financial institution or one or more other institutions that hold ownership or servicing rights in conjunction with the financial institution hires an agent to collect on the loan.

(b) Consumer does not include an individual who:

(1) is a consumer of another financial institution that uses a different financial institution to act solely as an agent for, or provide processing or other services to, the consumer's financial institution;

(2) designates a financial institution solely for the purposes to act as a trustee for a trust;

(3) is the beneficiary of a trust for which the financial institution serves as trustee; or

(4) is a participant or a beneficiary of an employee benefit plan that the financial institution sponsors or for which the financial institution acts as a trustee or fiduciary.

Subd. 5. **Continuing relationship.** (a) "Continuing relationship" means a consumer:

(1) has a credit or investment account with a financial institution;

(2) obtains a loan from a financial institution;

(3) purchases an insurance product from a financial institution;

(4) holds an investment product through a financial institution, including but not limited to when the financial institution acts as a custodian for securities or for assets in an individual retirement arrangement;

(5) enters into an agreement or understanding with a financial institution whereby the financial institution 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 institution;

(7) obtains financial, investment, or economic advisory services from a financial institution for a fee;

(8) becomes a financial institution's client to obtain tax preparation or credit counseling services from the financial institution;

(9) obtains career counseling while: (i) seeking employment with a financial institution or the finance, accounting, or audit department of any company; or (ii) employed by a financial institution or department of any company;

(10) is obligated on an account that a financial institution purchases from another financial institution, regardless of whether the account is in default when purchased, unless the financial institution 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 institution; or

(12) has a loan for which a financial institution owns the servicing rights.

(b) Continuing relationship does not include situations where:

(1) the consumer obtains a financial product or service from a financial institution only in isolated transactions, including but not limited to: (i) using a financial institution's automated teller machine to withdraw cash from an account at another financial institution; (ii) purchasing a money order from a financial institution; (iii) cashing a check with a financial institution; or (iv) making a wire transfer through a financial institution;

(2) a financial institution sells the consumer's loan and does not retain the rights to service the loan;

(3) a financial institution sells the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(4) the consumer obtains onetime personal or real property appraisal services from a financial institution; or

(5) the consumer purchases checks for a personal checking account from a financial institution.

Subd. 6. **Customer.** "Customer" means a consumer who has a customer relationship with a financial institution.

Subd. 7. **Customer information.** "Customer information" means any record containing nonpublic personal information about a financial institution's customer, whether the record is in paper, electronic, or another form, that is handled or maintained by or on behalf of the financial institution or the financial institution's affiliates.

Subd. 8. **Customer relationship.** "Customer relationship" means a continuing relationship between a consumer and a financial institution under which the financial institution provides to the consumer one or more financial products or services that are used primarily for personal, family, or household purposes.

Subd. 9. **Encryption.** "Encryption" means the transformation of data into a format 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.

Subd. 10. **Financial product or service.** "Financial product or service" means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956, United States Code, title 12, section 1843(k). Financial product or service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

Subd. 11. **Financial institution.** "Financial institution" has the meaning given in or as used by: (1) chapters 48A, 53, 53A, 53B, 53C, 56, 58, 58B, 332A, or 332B; or (2) sections 47.60, 47.62, or 332.54.

Subd. 12. **Information security program.** "Information security program" means the administrative, technical, or physical safeguards a financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Subd. 13. **Information system.** "Information system" means a discrete set of electronic information resources organized to collect, process, maintain, use, share, disseminate, or dispose of electronic information, as well as any specialized system, including but not limited to industrial process controls systems, telephone switching and private branch exchange systems, and environmental controls systems, that contains customer information or that is connected to a system that contains customer information.

Subd. 14. **Multifactor authentication.** "Multifactor authentication" means authentication through verification of at least two of the following factors:

(1) knowledge factors, including but not limited to a password;

(2) possession factors, including but not limited to a token; or

(3) inherence factors, including but not limited to biometric characteristics.

Subd. 15. **Nonpublic personal information.** (a) "Nonpublic personal information" means:

(1) personally identifiable financial information; or

(2) any list, description, or other grouping of consumers, including publicly available information pertaining to the list, description, or other grouping of consumers, that is derived using personally identifiable financial information that is not publicly available.

(b) Nonpublic personal information includes but is not limited to any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, including account numbers.

(c) Nonpublic personal information does not include:

(1) publicly available information, except as included on a list described in paragraph (a), clause (2);

(2) any list, description, or other grouping of consumers, including publicly available information pertaining to the list, description, or other grouping of 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 institution's consumer.

Subd. 16. **Notification event.** "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 this purpose 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 institution has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of customer information.

Subd. 17. **Penetration testing.** "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 institution's information systems.

Subd. 18. **Personally identifiable financial information.** (a) "Personally identifiable financial information" means any information:

(1) a consumer provides to a financial institution to obtain a financial product or service;

(2) about a consumer resulting from any transaction involving a financial product or service between a financial institution and a consumer; or

(3) a financial institution otherwise obtains about a consumer in connection with providing a financial product or service to the customer.

(b) Personally identifiable financial information includes:

(1) information a consumer provides to a financial institution 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) the fact that an individual is or has been a financial institution's customer or has obtained a financial product or service from the financial institution;

(4) any information about a financial institution's consumer, if the information is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer;

(5) any information that a consumer provides to a financial institution or that a financial institution or a financial institution's agent otherwise obtains in connection with collecting on or servicing a credit account;

(6) any information a financial institution collects through an Internet information collecting device from a web server; and

(7) information from a consumer report.

(c) Personally identifiable financial information does not include:

(1) a list of customer names and addresses for an entity that is not a financial institution; and

(2) information that does not identify a consumer, including but not limited to aggregate information or blind data that does not contain personal identifiers, including account numbers, names, or addresses.

Subd. 19. **Publicly available information.** (a) "Publicly available information" means any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from:

(1) federal, state, or local government records;

(2) widely distributed media; or

(3) disclosures to the general public that are required under federal, state, or local law.

(b) Publicly available information includes but is not limited to:

(1) with respect to government records, information in government real estate records and security interest filings; and

(2) with respect to widely distributed media, information from 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 merely because an Internet service provider or a site operator requires a fee or a password, provided that access is available to the general public.

(c) For purposes of this subdivision, a financial institution has a reasonable basis to believe that information is lawfully made available to the general public if the financial

institution has taken steps to determine: (1) that the information is of the type that is 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 institution's consumer has not directed that the information not be made available to the general public. A financial institution has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the financial institution determines the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded. A financial institution has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the financial institution has located the telephone number in the telephone book or the consumer has informed the financial institution that the telephone number is not unlisted.

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

Subd. 21. **Security event.** "Security event" means an event resulting in unauthorized access to, or disruption or misuse of: (1) an information system or information stored on an information system; or (2) customer information held in physical form.

Subd. 22. **Service provider.** "Service provider" means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through the service provider's provision of services directly to a financial institution that is subject to this chapter.

Sec. 2. **[46A.02] SAFEGUARDING CUSTOMER INFORMATION; STANDARDS.**

Subdivision 1. **Information security program.** (a) A financial institution must develop, implement, and maintain a comprehensive information security program.

(b) The information security program must: (1) be written in one or more readily accessible parts; and (2) contain administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of the financial institution's activities, and the sensitivity of any customer information at issue.

(c) The information security program must include the elements set forth in section 46A.03 and must be reasonably designed to achieve the objectives of this chapter, as established under subdivision 2.

Subd. 2. **Objectives.** The objectives of this chapter 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 customer information; and

(3) protect against unauthorized access to or use of customer information that might result in substantial harm or inconvenience to a customer.

Sec. 3. **[46A.03] ELEMENTS.**

Subdivision 1. **Generally.** In order to develop, implement, and maintain an information security program, a financial institution must comply with this section.

Subd. 2. **Qualified individual.** (a) A financial institution must designate a qualified individual responsible for overseeing, implementing, and enforcing the financial institution's information security program. The qualified individual may be employed by the financial institution, an affiliate, or a service provider.

(b) If a financial institution designates an individual employed by an affiliate or service provider as the financial institution's qualified individual, the financial institution must:

(1) retain responsibility for complying with this chapter;

(2) designate a senior member of the financial institution's personnel to be responsible for directing and overseeing the qualified individual's activities; and

(3) require the service provider or affiliate to maintain an information security program that protects the financial institution in a manner that complies with the requirements of this chapter.

Subd. 3. **Security risk assessment.** (a) A financial institution must base the financial institution's information security program on a risk assessment that:

(1) identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that might result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information; and

(2) assesses the sufficiency of any safeguards in place to control the risks identified under clause (1).

(b) The risk assessment must be made in writing and must include:

(1) criteria to evaluate and categorize identified security risks or threats the financial institution faces;

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

(3) requirements describing how:

(i) identified risks are mitigated or accepted based on the risk assessment; and

(ii) the information security program addresses the risks.

(c) A financial institution must periodically perform additional risk assessments that:

(1) reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that might result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information; and

(2) reassess the sufficiency of any safeguards in place to control the risks identified under clause (1).

Subd. 4. **Risk control.** A financial institution must design and implement safeguards to control the risks the financial institution identifies through the risk assessment under subdivision 3, including by:

(1) implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) limit an authorized user's access to only customer information that the authorized user needs to perform the authorized user's duties and functions or, in the case of a customer, to limit access to the customer's own information;

(2) identifying and managing the data, personnel, devices, systems, and facilities that enable the financial institution to achieve business purposes in accordance with the business purpose's relative importance to business objectives and the financial institution's risk strategy;

(3) protecting by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest. To the extent a financial institution determines that encryption of customer information either in transit over external networks or at rest is infeasible, the financial institution may secure the customer information

using effective alternative compensating controls that have been reviewed and approved by the financial institution's qualified individual;

(4) adopting: (i) secure development practices for in-house developed applications utilized by the financial institution to transmit, access, or store customer information; and (ii) procedures to evaluate, assess, or test the security of externally developed applications the financial institution uses to transmit, access, or store customer information;

(5) implementing multifactor authentication for any individual that accesses any information system, unless the financial institution's qualified individual has approved in writing the use of a reasonably equivalent or more secure access control;

(6) 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 relates, unless the information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or if targeted disposal is not reasonably feasible due to the manner in which the information is maintained;

(7) periodically reviewing the financial institution's data retention policy to minimize the unnecessary retention of data;

(8) adopting procedures for change management; and

(9) implementing policies, procedures, and controls designed to: (i) monitor and log the activity of authorized users; and (ii) detect unauthorized access to, use of, or tampering with customer information by authorized users.

Subd. 5. **Testing and monitoring.** (a) A financial institution must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including the controls, systems, and procedures that detect actual and attempted attacks on, or intrusions into, information systems.

(b) For information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect on an ongoing basis any changes in information systems that may create vulnerabilities, a financial institution must conduct:

(1) annual penetration testing of the financial institution'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 institution's information systems based on the risk assessment, at least every six months, whenever a material change to the financial institution's operations or business arrangements occurs, and whenever the financial institution knows or has reason to know circumstances exist that may have a material impact on the financial institution's information security program.

Subd. 6. **Internal policies and procedures.** A financial institution must implement policies and procedures to ensure that the financial institution's personnel are able to enact the financial institution's information security program by:

(1) providing the financial institution's personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) utilizing qualified information security personnel employed by the financial institution, an affiliate, or a service provider sufficient to manage the financial institution's 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.

Subd. 7. **Provider oversight.** A financial institution must 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 by contract the financial institution's service providers to implement and maintain appropriate safeguards; and

(3) periodically assessing the financial institution's service providers based on the risk the service providers present and the continued adequacy of the service providers' safeguards.

Subd. 8. **Information security program; evaluation; adjustment.** A financial institution must evaluate and adjust the financial institution's information security program to reflect: (1) the results of the testing and monitoring required under subdivision 5; (2) any material changes to the financial institution's operations or business arrangements; (3) the results of risk assessments performed under subdivision 3, paragraph (c); or (4) any other circumstances that the financial institution knows or has reason to know may have a material impact on the financial institution's information security program.

Subd. 9. **Incident response plan.** A financial institution must 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 institution controls. An incident response plan must address:

(1) the goals of the incident response plan;

(2) the internal processes to respond to a security event;

(3) clear roles, responsibilities, and levels of decision making authority;

(4) external and internal communications and information sharing;

(5) requirements to remediate any identified weaknesses in information systems and associated controls;

(6) documentation and reporting regarding security events and related incident response activities; and

(7) evaluation and revision of the incident response plan as necessary after a security event.

Subd. 10. **Annual report.** (a) A financial institution must require the financial institution's qualified individual to report at least annually in writing to the financial institution's board of directors or equivalent governing body. If a board of directors or equivalent governing body does not exist, the report under this subdivision must be timely presented to a senior officer responsible for the financial institution's information security program.

(b) The report made under this subdivision must include the following information:

(1) the overall status of the financial institution's information security program, including compliance with this chapter and associated administrative rules; and

(2) material matters related to the financial institution's information security program, including but not limited to addressing issues pertaining to: (i) the risk assessment; (ii) risk management and control decisions; (iii) service provider arrangements; (iv) testing results; (v) security events or violations and management's responses to the security event or violation; and (vi) recommendations for changes in the information security program.

Subd. 11. **Business continuity; disaster recovery.** A financial institution must establish a written plan addressing business continuity and disaster recovery.

Sec. 4. **[46A.04] EXCEPTIONS.**

Section 46A.03, subdivisions 3; 5, paragraph (b); 9; and 10, do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.

Sec. 5. **[46A.05] ALTERATION OF FEDERAL REGULATION.**

(a) If an amendment to Code of Federal Regulations, title 16, part 314, results in a complete lack of federal regulations in the area, the version of the state requirements in effect at the time of the amendment remain in effect for two years from the date the amendment becomes effective.

(b) During the time period under paragraph (a), the department must adopt replacement administrative rules as necessary and appropriate.

Sec. 6. **[46A.06] NOTIFICATION EVENT.**

Subdivision 1. **Notification requirement.** (a) Upon discovering a notification event as described in subdivision 2, if the notification event involves the information of at least 500 consumers, a financial institution must notify the commissioner as soon as possible, but no later than 30 days after the date the event is discovered. The notice must be made (1) in a format specified by the commissioner, and (2) electronically on a form located on the department's website.

(b) The notice must include:

(1) the name and contact information of the reporting financial institution;

(2) a description of the types of information involved in the notification event;

(3) if possible to determine, the date or date range of the notification event;

(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 (i) disclosing whether a law enforcement official has provided the financial institution with a written determination indicating that providing notice to the public regarding the breach would impede a criminal investigation or cause damage to national security, and (ii) if a written determination described under item (i) was provided to the financial institution, providing contact information that enables the commissioner to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date that notice was provided to the commissioner. The delay may be

extended for an additional period of up to 60 days if the law enforcement official seeks an extension in writing. An additional delay may be permitted only if the commissioner determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

Subd. 2. **Notification event treated as discovered.** A notification event must be treated as discovered on the first day when the event is known to a financial institution. A financial institution is deemed to have knowledge of a notification event if the event is known to any person, other than the person committing the breach, who is the financial institution's employee, officer, or other agent.

Sec. 7. **[46A.07] COMMISSIONER'S POWERS.**

(a) The commissioner has the power to examine and investigate the affairs of any covered financial institution to determine whether the financial institution has been or is engaged in any conduct that violates this chapter. This power is in addition to the powers granted to the commissioner under section 46.01.

(b) If the commissioner has reason to believe that a financial institution has been or is engaged in conduct in Minnesota that violates this chapter, the commissioner may take action necessary or appropriate to enforce this chapter."

Renumber the sections in sequence and correct the internal references

Amend the title accordingly