A bill to be entitled

An act relating to the Office of Financial Regulation; creating s. 494.00123, F.S.; providing definitions; requiring loan originators, mortgage brokers, and mortgage lenders to develop, implement, and maintain comprehensive written information security programs for the protection of information systems and nonpublic personal information; providing requirements for such programs; requiring loan originators, mortgage brokers, and mortgage lenders to establish written incident response plans for specified purposes; providing requirements for such plans; providing applicability; providing compliance requirements under specified circumstances; requiring loan originators, mortgage brokers, and mortgage lenders to maintain copies of information security programs for a specified timeframe and to make them available to the Office of Financial Regulation under certain circumstances; requiring loan originators, mortgage brokers, and mortgage lenders and certain entities to conduct investigations of cybersecurity events under certain circumstances; providing requirements for such investigations; providing requirements for records and documentation maintenance; providing requirements for notices of security breaches; providing construction; providing rulemaking authority; amending s. 494.00255, F.S.; providing additional acts that constitute a ground for specified disciplinary actions against loan originators and mortgage brokers; amending s. 517.021, F.S.; revising the definition of the term "investment adviser" and defining the term "place of business"; amending s. 559.952, F.S.; revising definitions; removing the definition of the term "innovative"; revising the list of general law provisions that are waived upon approval of a Financial Technology Sandbox application; revising conditions under which a waiver of a requirement may be granted; providing that provisions applicable to the Financial Technology Sandbox innovative financial products and services apply to Financial Technology Sandbox financial products and services; revising the criteria for the office to consider when deciding whether to approve or deny an application for licensure; authorizing, rather than requiring, the office to specify the maximum number of consumers authorized to receive financial products and services from a Financial Technology Sandbox applicant; removing provisions that limit the number of such customers; revising construction; amending s. 560.114, F.S.; specifying the entities that are subject to certain disciplinary actions and penalties; revising the list of actions by money services businesses which constitute grounds for certain disciplinary actions and penalties; requiring, rather than authorizing, the office to suspend licenses of money services businesses under certain circumstances; s. 560.1311, F.S.; providing definitions; requiring money services businesses to develop, implement, and maintain comprehensive written information security programs for the protection of information systems and nonpublic personal information; providing requirements for such programs; requiring money services businesses to establish written incident response plans for specified purposes; providing requirements for such plans; providing applicability; providing compliance requirements under specified circumstances; requiring money services businesses to maintain copies of information security programs for a specified timeframe and to make them available to the office under certain circumstances; requiring money services businesses and certain entities to conduct investigations of cybersecurity events under certain circumstances; providing requirements for such investigations; providing requirements for records and documentation maintenance; providing requirements for notices of security breaches; providing construction; providing rulemaking authority; creating s. 655.0171, F.S.; providing definitions; requiring financial institutions to take measures to protect and secure certain data that contain personal information; providing requirements for notices of security breaches to the office, the Department of Legal Affairs, certain individuals, and certain credit reporting agencies; amending s. 655.045, F.S.; revising the timeline for the mailing of payment for salary and travel expenses of certain field staff; amending s. 657.005, F.S.; revising requirements for permission to organize credit unions; amending s. 657.024, F.S.; authorizing meetings of credit union members to be held virtually and without quorums under certain circumstances; amending s. 657.042, F.S.; removing provisions that impose limitations on investments in real estate and equipment for credit unions; amending s. 658.21, F.S.; revising requirements and factors for approving applications for organizing banks and trust companies; amending s. 658.33, F.S.; revising requirements for directors of certain banks and trust companies; amending s. 662.141, F.S.; revising the timeline for the mailing of payment for the salary and travel expenses of certain field staff; amending s. 517.12, F.S.; conforming a cross-reference; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 494.00123, Florida Statutes, is created to read:

494.00123 Information security programs; cybersecurity event investigations.—

(1) DEFINITIONS.—As used in this section, the term:

(a) "Customer" means a person who seeks to obtain or who obtains or has obtained a financial product or service from a licensee.

(b) "Customer information" means any record containing nonpublic personal information about a customer of a financial transaction, whether on paper, electronic, or in other forms, which is handled or maintained by or on behalf of the licensee or its affiliates.

(c) "Cybersecurity event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

(d) "Financial product or service" means any product or service offered by a licensee under this chapter.

(e) "Information security program" means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(f) "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 an industrial process control system, telephone switching and private branch exchange system, or environmental control system, which contain customer information or which are connected to a system that contains customer information.

(g) "Licensee" means a person licensed under this chapter.

(h)1. "Nonpublic personal information" means:

a. Personally identifiable financial information; and

b. Any list, description, or other grouping of customers that is derived using any personally identifiable financial information that is not publicly available, such as account numbers, including 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.

2. The term does not include:

a. Publicly available information, except as included on a list, description, or other grouping of customers described in sub-subparagraph 1.b.;

b. Any list, description, or other grouping of consumers, or any publicly available information pertaining to such list, description, or other grouping of consumers, which is derived without using any personally identifiable financial information that is not publicly available; or

c. 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 of the individuals on the list is a customer of a licensee.

3. As used in this paragraph, the term:

a.(I) "Personally identifiable financial information" means any information that:

(A) A customer provides to a licensee to obtain a financial product or service, such as information that a customer provides to a licensee on an application to obtain a loan or other financial product or service;

(B) A licensee receives about a consumer that is obtained during or as a result of any transaction involving a financial product or service between the licensee and the customer, such as information collected through an information-collecting device from a web server; or

(C) A licensee otherwise obtains about a customer in connection with providing a financial product or service to the customer, such as the fact that an individual is or has been one of the licensee's customers or has obtained a financial product or service from the licensee.

(II) The term "personally identifiable financial information" does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; or

(B) Information that does not identify a customer, such as blind data or aggregate information that does not contain personal identifiers such as account numbers, names, or addresses.

b.(I) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(A) Federal, state, or local government records, such as government real estate records or security interest filings;

(B) Widely distributed media, such as information from a telephone records repository or directory, a television or radio program, a newspaper, a social media platform, 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, so long as access is available to the general public; or

(C) Disclosures to the general public which are required to be made by federal, state, or local law.

(II) As used in this sub-subparagraph, the term "reasonable basis to believe is lawfully made available to the general public" relating to any information means that the person has taken steps to determine:

(A) That the information is of the type that is available to the general public, such as information included on the public record in the jurisdiction where the mortgage would be recorded; and

(B) Whether an individual can direct that the information not be made available to the general public and, if so, the customer to whom the information relates has not done so, such as when a telephone number is listed in a telephone directory and the customer has informed the licensee that the telephone number is not unlisted.

(i) "Third-party service provider" means a person, other than a licensee, which contracts with a licensee to maintain, process, or store nonpublic personal information, or is otherwise permitted access to nonpublic personal information through its provision of services to a licensee.

(2) INFORMATION SECURITY PROGRAM.—

(a) Each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of the licensee's information system and nonpublic personal information.

(b) Each licensee shall ensure that the information security program meets all of the following criteria:

1. Be commensurate with the following measures:

a. Size and complexity of the licensee.

b. Nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

c. Sensitivity of nonpublic personal information that is used by the licensee or that is in the licensee's possession, custody, or control.

2. Be designed to do all of the following:

a. Protect the security and confidentiality of nonpublic personal information and the security of the licensee's information system.

b. Protect against threats or hazards to the security or integrity of nonpublic personal information and the licensee's information system.

c. Protect against unauthorized access to or the use of nonpublic personal information and minimize the likelihood of harm to any customer.

3. Define and periodically reevaluate the retention schedule and the mechanism for the destruction of nonpublic personal information if retention is no longer necessary for the

licensee's business operations or is no longer required by applicable law.

4. Regularly test and monitor systems and procedures for the detection of actual and attempted attacks on, or intrusions into, the licensee's information system.

5. Be monitored, evaluated, and adjusted, as necessary, to meet all of the following requirements:

a. Determine whether the licensee's information security program is consistent with relevant changes in technology.

b. Confirm the licensee's information security program accounts for the sensitivity of nonpublic personal information.

c. Identify changes that may be necessary to the licensee's information system.

d. Eliminate any internal or external threats to nonpublic personal information.

e. Amend the licensee's information security program for any of the licensee's changing business arrangements, including, but not limited to, mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements.

(c)1. As part of a licensee's information security program, the licensee shall establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises:

a. The confidentiality, integrity, or availability of nonpublic personal information in the licensee's possession;

b. The licensee's information system; or

c. The continuing functionality of any aspect of the licensee's operations.

2. The written incident response plan must address all of the following:

a. The licensee's internal process for responding to a cybersecurity event.

b. The goals of the licensee's incident response plan.

c. The assignment of clear roles, responsibilities, and levels of decisionmaking authority for the licensee's personnel that participate in the incident response plan.

d. External communications, internal communications, and information sharing related to a cybersecurity event.

e. The identification of remediation requirements for weaknesses identified in information systems and associated controls.

f. The documentation and reporting regarding cybersecurity events and related incident response activities.

g. The evaluation and revision of the incident response plan, as appropriate, following a cybersecurity event.

h. The process by which notice must be given as required under subsection (4) and s. 501.171(3) and (4).

(d)1. This section does not apply to a licensee that has fewer than:

a. Twenty individuals on its workforce, including employees and independent contractors; or

b. Five hundred customers during a calendar year.

2. A licensee that no longer qualifies for exemption under subparagraph 1. has 180 calendar days to comply with this section after the date of the disqualification.

(e) Each licensee shall maintain a copy of the information security program for a minimum of 5 years and shall make it available to the office upon request or as part of an examination.

(3) CYBERSECURITY EVENT INVESTIGATION.—

(a) If a licensee discovers that a cybersecurity event has occurred or that a cybersecurity event may have occurred, the licensee, or an outside vendor or third-party service provider that the licensee has designated to act on its behalf, shall conduct a prompt investigation of the cybersecurity event.

(b) During the investigation, the licensee, or the outside vendor or third-party service provider that the licensee has designated to act on its behalf, shall, at a minimum, determine as much of the following as possible:

1. Confirm that a cybersecurity event has occurred.

2. Identify the date that the cybersecurity event first occurred.

3. Assess the nature and scope of the cybersecurity event.

4. Identify all nonpublic personal information that may have been compromised by the cybersecurity event.

5. Perform or oversee reasonable measures to restore the security of any compromised information system in order to prevent further unauthorized acquisition, release, or use of nonpublic personal information that is in the licensee's, outside vendor's, or third-party service provider's possession, custody, or control.

(c) If a licensee learns that a cybersecurity event has occurred, or may have occurred, in an information system maintained by a third-party service provider of the licensee, the licensee shall complete an investigation in compliance with this section or confirm and document that the third-party service provider has completed an investigation in compliance with this section.

(d) A licensee shall maintain all records and documentation related to the licensee's investigation of a cybersecurity event for a minimum of 5 years after the date of the cybersecurity event and shall produce the records and documentation to the office upon request.

(4) NOTICE TO OFFICE OF SECURITY BREACH.—

(a) Each licensee shall provide notice to the office of any breach of security affecting 500 or more individuals in this state at a time and in the manner prescribed by commission rule.

(b) Each licensee shall, upon the office's request, provide a quarterly update of a cybersecurity event investigation under subsection (3) until conclusion of the

<u>investigation.</u>

<u>(5) CONSTRUCTION.—This section may not be construed to relieve a covered entity from complying with s. 501.171. To the extent a licensee is a covered entity, as defined in s. 501.171(1), the licensee remains subject to s. 501.171.</u>

<u>(6) RULES.—The commission may adopt rules to administer this section, including rules that allow a licensee that is in full compliance with the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 C.F.R. part 314, to be deemed in compliance with subsection (2).</u>

Section 2. Paragraph (z) is added to subsection (1) of section 494.00255, Florida Statutes, to read:

494.00255 Administrative penalties and fines; license violations.—

(1) Each of the following acts constitutes a ground for which the disciplinary actions specified in subsection (2) may be taken against a person licensed or required to be licensed under part II or part III of this chapter:

<u>(z) Failure to comply with the notification requirements in s. 501.171(3) and (4).</u>

Section 3. Subsections (28) through (36) of section 517.021, Florida Statutes, are renumbered as subsections (29) through (37), respectively, subsection (20) is amended, and a new subsection (28) is added to that section, to read:

517.021 Definitions.—When used in this chapter, unless the context otherwise indicates, the following terms have the following respective meanings:

(20)(a) "Investment adviser" means a person, other than an associated person of an investment adviser or a federal covered adviser, that receives compensation, directly or indirectly, and engages for all or part of the person's time, directly or indirectly, or through publications or writings, in the business of advising others as to the value of securities or as to the advisability of investments in, purchasing of, or selling of securities.

(b) The term does not include any of the following:

1. A dealer or an associated person of a dealer whose performance of services in paragraph (a) is solely incidental to the conduct of the dealer's or associated person's business as a dealer and who does not receive special compensation for those services.

2. A licensed practicing attorney or certified public accountant whose performance of such services is solely incidental to the practice of the attorney's or accountant's profession.

3. A bank authorized to do business in this state.

4. A bank holding company as defined in the Bank Holding Company Act of 1956, as amended, authorized to do business in this state.

5. A trust company having trust powers, as defined in s.

658.12, which it is authorized to exercise in this state, which trust company renders or performs investment advisory services in a fiduciary capacity incidental to the exercise of its trust powers.

6. A person that renders investment advice exclusively to insurance or investment companies.

7. A person:

a. Without a place of business in this state if the person has had ~~that~~, during the preceding 12 months, ~~has~~ fewer than six clients who are residents of this state.

b. With a place of business in this state if the person has had, during the preceding 12 months, fewer than six clients who are residents of this state and no clients who are not residents of this state.

As used in this subparagraph, the term "client" has the same meaning as provided in Securities and Exchange Commission Rule 222-2 ~~275.222-2~~, 17 C.F.R. s. 275.222-2, as amended.

8. A federal covered adviser.

9. The United States, a state, or any political subdivision of a state, or any agency, authority, or instrumentality of any such entity; a business entity that is wholly owned directly or indirectly by such a governmental entity; or any officer, agent, or employee of any such governmental or business entity who is acting within the scope

of his or her official duties.

10. A family office as defined in Securities and Exchange Commission Rule 202(a)(11)(G)-1(b) and (d) under the Investment Advisers Act of 1940, 17 C.F.R. s. 275. 202(a)(11)(G)-1(b) and (d), as amended, without giving regard to paragraph 1(a) or paragraph 1(c) of that rule.

(28) "Place of business" of an investment adviser means an office at which the investment adviser regularly provides investment advisory services, solicits, meets with, or otherwise communicates with clients; and any other location that is held out to the general public as a location at which the investment adviser provides investment advisory services, solicits, meets with, or otherwise communicates with clients.

Section 4. Section 559.952, Florida Statutes, is amended to read:

559.952 Financial Technology Sandbox.—

(1) SHORT TITLE.—This section may be cited as the "Financial Technology Sandbox."

(2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—There is created the Financial Technology Sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox using ~~exceptions to specified general law and~~ waivers of specified provisions of general law and the corresponding rule requirements under defined conditions. The

creation of a supervised, flexible regulatory sandbox provides a welcoming business environment for technology innovators and may lead to significant business growth.

(3) DEFINITIONS.—As used in this section, the term:

(a) "Business entity" means any corporation, limited liability company, or trust that may or may not be fictitiously named and that does business in this state ~~a domestic corporation or other organized domestic entity with a physical presence, other than that of a registered office or agent or virtual mailbox, in this state~~.

(b) "Commission" means the Financial Services Commission.

(c) "Consumer" means a person in this state, whether a natural person or a business organization, who purchases, uses, receives, or enters into an agreement to purchase, use, or receive a ~~an innovative~~ financial product or service made available through the Financial Technology Sandbox.

(d) "Control person" means an individual, a partnership, a corporation, a trust, or other organization that possesses the power, directly or indirectly, to direct the management or policies of a company, whether through ownership of securities, by contract, or through other means. A person is presumed to control a company if, with respect to a particular company, that person:

1. Is a director, a general partner, or an officer exercising executive responsibility or having similar status or

functions;

2. Directly or indirectly may vote 10 percent or more of a class of a voting security or sell or direct the sale of 10 percent or more of a class of voting securities; or

3. In the case of a partnership, may receive upon dissolution or has contributed 10 percent or more of the capital.

(e) "Corresponding rule requirements" means the commission rules, or portions thereof, which implement the general laws enumerated in paragraph (4)(a).

(f) "Financial product or service" means a product or service related to ~~a~~ consumer finance ~~loan, as defined in s. 516.01,~~ or credit, banking services, money transmission, or securities transactions ~~a money transmitter or payment instrument seller, as those terms are defined in s. 560.103, including mediums of exchange that are in electronic or digital form,~~ which is subject to the general laws enumerated in paragraph (4)(a) and corresponding rule requirements and which is under the jurisdiction of the office.

(g) "Financial Technology Sandbox" means the program created by this section which allows a licensee to make a ~~an innovative~~ financial product or service available to consumers during a sandbox period through waivers of ~~exceptions to~~ general laws and ~~waivers of~~ corresponding rule requirements.

~~(h) "Innovative" means new or emerging technology, or new~~

~~uses of existing technology, which provide a product, service, business model, or delivery mechanism to the public and which are not known to have a comparable offering in this state outside the Financial Technology Sandbox.~~

(h) ~~(i)~~ "Licensee" means a business entity that has been approved by the office to participate in the Financial Technology Sandbox.

(i) ~~(j)~~ "Office" means, unless the context clearly indicates otherwise, the Office of Financial Regulation.

(j) ~~(k)~~ "Sandbox period" means the initial 24-month period in which the office has authorized a licensee to make a ~~an innovative~~ financial product or service available to consumers, and any extension granted pursuant to subsection (7).

(4) WAIVERS OF ~~EXCEPTIONS TO~~ GENERAL LAW AND CORRESPONDING ~~WAIVERS OF~~ RULE REQUIREMENTS.—

(a) Notwithstanding any other law, upon approval of a Financial Technology Sandbox application, the office may grant an applicant during a sandbox period a waiver of a requirement, or a portion thereof, imposed by a general law or rule in any following chapter, or part thereof, if all of the conditions in paragraph (b) are met ~~following provisions and corresponding rule requirements are not applicable to the licensee during the sandbox period~~:

1. Chapter 516, Consumer Finance.

2. Chapter 517, Securities Transactions.

3. Chapter 520, Retail Installment Sales.

4. Chapter 537, Title Loans.

5. Part I or part II of chapter 560, General Provisions of Money Services Businesses or Payment Instruments and Funds Transmission.

6. Chapter 655, Financial Institutions Generally.

7. Chapter 657, Credit Unions.

8. Chapter 658, Banks and Trust Companies.

9. Chapter 660, Trust Business.

10. Chapter 662, Family Trust Companies.

11. Chapter 663, International Banking.

~~1. Section 516.03(1), except for the application fee, the investigation fee, the requirement to provide the social security numbers of control persons, evidence of liquid assets of at least $25,000 or documents satisfying the requirements of s. 516.05(10), and the office's authority to investigate the applicant's background. The office may prorate the license renewal fee for an extension granted under subsection (7).~~

~~2. Section 516.05(1) and (2), except that the office shall investigate the applicant's background.~~

~~3. Section 560.109, only to the extent that the section requires the office to examine a licensee at least once every 5 years.~~

~~4. Section 560.118(2).~~

~~5. Section 560.125(1), only to the extent that the~~

~~subsection would prohibit a licensee from engaging in the business of a money transmitter or payment instrument seller during the sandbox period.~~

~~6. Section 560.125(2), only to the extent that the subsection would prohibit a licensee from appointing an authorized vendor during the sandbox period. Any authorized vendor of such a licensee during the sandbox period remains liable to the holder or remitter.~~

~~7. Section 560.128.~~

~~8. Section 560.141, except for s. 560.141(1)(a)1., 3., 7.-10. and (b), (c), and (d).~~

~~9. Section 560.142(1) and (2), except that the office may prorate, but may not entirely eliminate, the license renewal fees in s. 560.143 for an extension granted under subsection (7).~~

~~10. Section 560.143(2), only to the extent necessary for proration of the renewal fee under subparagraph 9.~~

~~11. Section 560.204(1), only to the extent that the subsection would prohibit a licensee from engaging in, or advertising that it engages in, the activity of a payment instrument seller or money transmitter during the sandbox period.~~

~~12. Section 560.205(2).~~

~~13. Section 560.208(2).~~

~~14. Section 560.209, only to the extent that the office~~

~~may modify, but may not entirely eliminate, the net worth, corporate surety bond, and collateral deposit amounts required under that section. The modified amounts must be in such lower amounts that the office determines to be commensurate with the factors under paragraph (5)(c) and the maximum number of consumers authorized to receive the financial product or service under this section.~~

(b) The office may grant an applicant during a sandbox period a waiver of a requirement, or a portion thereof, imposed by a general law or rule in any chapter enumerated in paragraph (a) if all of the following conditions are met: ~~approve a Financial Technology Sandbox application if one or more of the general laws enumerated in paragraph (a) currently prevent the innovative financial product or service from being made available to consumers and if all other requirements of this section are met.~~

1. The general law or rule does not currently authorize the financial product or service to be made available to consumers.

2. The waiver is not broader than necessary to accomplish the purposes and standards specified in this section, as determined by the office.

3. Any provision relating to the liability of an incorporator, director, or officer of the applicant is not eligible for a waiver.

(c) A licensee may conduct business through electronic means, including through the Internet or a software application.

(5) FINANCIAL TECHNOLOGY SANDBOX APPLICATION; STANDARDS FOR APPROVAL.—

(a) Before filing an application for licensure under this section, a substantially affected person may seek a declaratory statement pursuant to s. 120.565 regarding the applicability of a statute, a rule, or an agency order to the petitioner's particular set of circumstances or a variance or waiver of a rule pursuant to s. 120.542.

(b) Before making a ~~an innovative~~ financial product or service available to consumers in the Financial Technology Sandbox, a business entity must file with the office an application for licensure under the Financial Technology Sandbox. The commission shall, by rule, prescribe the form and manner of the application and how the office will evaluate and apply each of the factors specified in paragraph (c).

1. The application must specify each general law enumerated in paragraph (4)(a) which currently prevents the ~~innovative~~ financial product or service from being made available to consumers and the reasons why those provisions of general law prevent the ~~innovative~~ financial product or service from being made available to consumers.

2. The application must contain sufficient information for the office to evaluate the factors specified in paragraph (c).

3. An application submitted on behalf of a business entity must include evidence that the business entity has authorized the person to submit the application on behalf of the business entity intending to make a ~~an innovative~~ financial product or service available to consumers.

4. The application must specify the maximum number of consumers, which may not exceed the number of consumers specified in paragraph (f), to whom the applicant proposes to provide the ~~innovative~~ financial product or service.

5. The application must include a proposed draft of the statement or statements meeting the requirements of paragraph (6)(b) which the applicant proposes to provide to consumers.

(c) The office shall approve or deny in writing a Financial Technology Sandbox application within 60 days after receiving the completed application. The office and the applicant may jointly agree to extend the time beyond 60 days. Consistent with this section, the office may impose conditions on any approval. In deciding whether to approve or deny an application for licensure, the office must consider each of the following:

1. The nature of the ~~innovative~~ financial product or service proposed to be made available to consumers in the Financial Technology Sandbox, including all relevant technical details.

~~2. The potential risk to consumers and the methods that~~

~~will be used to protect consumers and resolve complaints during the sandbox period.~~

2.~~3.~~ The business plan proposed by the applicant, including company information~~, market analysis, and financial projections or pro forma financial statements, and evidence of the financial viability of the applicant~~.

~~4. Whether the applicant has the necessary personnel, adequate financial and technical expertise, and a sufficient plan to test, monitor, and assess the innovative financial product or service.~~

3.~~5.~~ Whether any control person of the applicant, regardless of adjudication, has pled no contest to, has been convicted or found guilty of, or is currently under investigation for fraud, a state or federal securities violation, a property-based offense, or a crime involving moral turpitude or dishonest dealing, in which case the application to the Financial Technology Sandbox must be denied.

4.~~6.~~ A copy of the disclosures that will be provided to consumers under paragraph (6)(b).

5.~~7.~~ The financial responsibility of the applicant and any control person, including whether the applicant or any control person has a history of unpaid liens, unpaid judgments, or other general history of nonpayment of legal debts, including, but not limited to, having been the subject of a petition for bankruptcy under the United States Bankruptcy Code within the past 7 calendar years.

6.~~8.~~ Any other factor that the office determines to be relevant.

(d) The office may not approve an application if:

1. The applicant had a prior Financial Technology Sandbox application that was approved and that related to a substantially similar financial product or service;

2. Any control person of the applicant was substantially involved in the development, operation, or management with another Financial Technology Sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service; or

3. The applicant or any control person has failed to affirmatively demonstrate financial responsibility.

(e) Upon approval of an application, the office shall notify the licensee of the specific ~~that the licensee is exempt from the~~ provisions of general law ~~enumerated in paragraph (4)(a)~~ and the corresponding rule requirements that are waived during the sandbox period. The office shall post on its website notice of the approval of the application, a summary of the ~~innovative~~ financial product or service, and the contact information of the licensee.

(f) The office, on a case-by-case basis, may ~~shall~~ specify the maximum number of consumers authorized to receive a ~~an innovative~~ financial product or service, after consultation with the Financial Technology Sandbox applicant. ~~The office may not authorize more than 15,000 consumers to receive the financial product or service until the licensee has filed the first report required under subsection (8). After the filing of that report, if the licensee demonstrates adequate financial capitalization, risk management processes, and management oversight, the office may authorize up to 25,000 consumers to receive the financial product or service.~~

(g) A licensee has a continuing obligation to promptly inform the office of any material change to the information provided under paragraph (b).

(h) The following information provided to and held by the office in a Financial Technology Sandbox application under this subsection is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

1. The reasons why a general law enumerated in paragraph (4)(a) prevents the ~~innovative~~ financial product or service from being made available to consumers.

2. The information provided for evaluation of the factors specified in subparagraphs (c)1. and 2. ~~3.~~

~~3. The information provided for evaluation of whether the applicant has a sufficient plan to test, monitor, and assess the innovative financial product or service, under subparagraph (c)~~4.

However, the confidential and exempt information may be released to appropriate state and federal agencies for the purposes of investigation. Nothing in this paragraph shall be construed to prevent the office from disclosing a summary of the ~~innovative~~ financial product or service.

(6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—

(a) A licensee may make a ~~an innovative~~ financial product or service available to consumers during the sandbox period.

(b)1. Before a consumer purchases, uses, receives, or enters into an agreement to purchase, use, or receive a ~~an innovative~~ financial product or service through the Financial Technology Sandbox, the licensee must provide a written statement of all of the following to the consumer:

a. The name and contact information of the licensee.

b. That the financial product or service has been authorized to be made available to consumers for a temporary period by the office, under the laws of this state.

c. That the state does not endorse the financial product or service.

d. That the financial product or service is undergoing testing, may not function as intended, and may entail financial risk.

e. That the licensee is not immune from civil liability for any losses or damages caused by the financial product or service.

f. The expected end date of the sandbox period.

g. The contact information for the office and notification that suspected legal violations, complaints, or other comments related to the financial product or service may be submitted to the office.

h. Any other statements or disclosures required by rule of the commission which are necessary to further the purposes of this section.

2. The written statement under subparagraph 1. must contain an acknowledgment from the consumer, which must be retained for the duration of the sandbox period by the licensee.

(c) The office may enter into an agreement with a state, federal, or foreign regulatory agency to allow licensees under the Financial Technology Sandbox to make their products or services available in other jurisdictions. The commission shall adopt rules to implement this paragraph.

(d) The office may examine the records of a licensee at any time, with or without prior notice.

(7) EXTENSION AND CONCLUSION OF SANDBOX PERIOD.—

(a) A licensee may apply for one extension of the initial 24-month sandbox period for 12 additional months for a purpose specified in subparagraph (b)1. or subparagraph (b)2. A complete application for an extension must be filed with the office at least 90 days before the conclusion of the initial sandbox period. The office shall approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period. In determining whether to approve or deny an application for extension of the sandbox period, the office must, at a minimum, consider the current status of the factors previously considered under paragraph (5)(c).

(b) An application for an extension under paragraph (a) must cite one of the following reasons as the basis for the application and must provide all relevant supporting information:

1. Amendments to general law or rules are necessary to offer the ~~innovative~~ financial product or service in this state permanently.

2. An application for a license that is required in order to offer the ~~innovative~~ financial product or service in this state permanently has been filed with the office and approval is pending.

(c) At least 30 days before the conclusion of the initial 24-month sandbox period or the extension, whichever is later, a licensee shall provide written notification to consumers regarding the conclusion of the initial sandbox period or the extension and may not make the financial product or service available to any new consumers after the conclusion of the initial sandbox period or the extension, whichever is later, until legal authority outside of the Financial Technology Sandbox exists for the licensee to make the financial product or service available to consumers. After the conclusion of the sandbox period or the extension, whichever is later, the business entity formerly licensed under the Financial Technology Sandbox may:

1. Collect and receive money owed to the business entity or pay money owed by the business entity, based on agreements with consumers made before the conclusion of the sandbox period or the extension.

2. Take necessary legal action.

3. Take other actions authorized by commission rule which are not inconsistent with this section.

(8) REPORT.—A licensee shall submit a report to the office twice a year as prescribed by commission rule. The report must, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

(9) CONSTRUCTION.—A business entity whose Financial Technology Sandbox application is approved under this section:

(a) Shall be deemed to possess an appropriate license under any general law requiring state licensure or authorization.

(b) Does not obtain a property right.

(c) Is not, nor is its financial product or service, endorsed by this state, nor is this state subject to liability for losses or damages caused by the financial product or service.

~~(a) Is licensed under chapter 516, chapter 560, or both chapters 516 and 560, as applicable to the business entity's activities.~~

~~(b) Is subject to any provision of chapter 516 or chapter 560 not specifically excepted under paragraph (4)(a), as applicable to the business entity's activities, and must comply with such provisions.~~

~~(c) May not engage in activities authorized under part III of chapter 560, notwithstanding s. 560.204(2).~~

(10) VIOLATIONS AND PENALTIES.—

(a) A licensee who makes a ~~an innovative~~ financial product or service available to consumers in the Financial Technology Sandbox remains subject to:

1. Civil damages for acts and omissions arising from or related to any ~~innovative~~ financial product or services provided or made available by the licensee or relating to this section.

2. All criminal and consumer protection laws and any other statute not specifically excepted under paragraph (4)(a).

(b)1. The office may, by order, revoke or suspend a licensee's approval to participate in the Financial Technology Sandbox if:

a. The licensee has violated or refused to comply with this section, any statute not specifically excepted under paragraph (4)(a), a rule of the commission that has not been waived, an order of the office, or a condition placed by the office on the approval of the licensee's Financial Technology Sandbox application;

b. A fact or condition exists that, if it had existed or become known at the time that the Financial Technology Sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;

c. A material error, false statement, misrepresentation, or material omission was made in the Financial Technology Sandbox application; or

d. After consultation with the licensee, the office determines that continued testing of the ~~innovative~~ financial product or service would:

(I) Be likely to harm consumers; or

(II) No longer serve the purposes of this section because of the financial or operational failure of the financial product or service.

2. Written notice of a revocation or suspension order made under subparagraph 1. must be served using any means authorized by law. If the notice relates to a suspension, the notice must include any condition or remedial action that the licensee must complete before the office lifts the suspension.

(c) The office may refer any suspected violation of law to an appropriate state or federal agency for investigation, prosecution, civil penalties, and other appropriate enforcement action.

(d) If service of process on a licensee is not feasible, service on the office is deemed service on the licensee.

(11) RULES AND ORDERS.—

(a) The commission shall adopt rules to administer this section before approving any application under this section.

(b) The office may issue all necessary orders to enforce this section and may enforce these orders in accordance with chapter 120 or in any court of competent jurisdiction. These orders include, but are not limited to, orders for payment of restitution for harm suffered by consumers as a result of a ~~an innovative~~ financial product or service.

Section 5. Subsections (1) and (2) of section 560.114, Florida Statutes, are amended to read:

560.114 Disciplinary actions; penalties.—

(1) The following actions by a money services business, an authorized vendor, or a ~~affiliated~~ party that was affiliated at the time of commission of the actions constitute grounds for the issuance of a cease and desist order; the issuance of a removal order; the denial, suspension, or revocation of a license; or taking any other action within the authority of the office pursuant to this chapter:

(a) Failure to comply with any provision of this chapter or related rule or order, or any written agreement entered into with the office.

(b) Fraud, misrepresentation, deceit, or gross negligence in any transaction by a money services business, regardless of reliance thereon by, or damage to, a customer.

(c) Fraudulent misrepresentation, circumvention, or concealment of any matter that must be stated or furnished to a customer pursuant to this chapter, regardless of reliance thereon by, or damage to, such customer.

(d) False, deceptive, or misleading advertising.

(e) Failure to maintain, preserve, keep available for examination, and produce all books, accounts, files, or other documents required by this chapter or related rules or orders, by 31 C.F.R. ss. 1010.306, 1010.311, 1010.312, 1010.340, 1010.410, 1010.415, 1022.210, 1022.320, 1022.380, and 1022.410, or by an agreement entered into with the office.

(f) Refusing to allow the examination or inspection of books, accounts, files, or other documents by the office pursuant to this chapter, or to comply with a subpoena issued by the office.

(g) Failure to pay a judgment recovered in any court by a claimant in an action arising out of a money transmission transaction within 30 days after the judgment becomes final.

(h) Engaging in an act prohibited under s. 560.111 or s. 560.1115.

(i) Insolvency.

(j) Failure by a money services business to remove an affiliated party after the office has issued and served upon the money services business a final order setting forth a finding that the affiliated party has violated a provision of this chapter.

(k) Making a material misstatement, misrepresentation, or omission in an application for licensure, any amendment to such application, or application for the appointment of an authorized vendor.

(l) Committing any act that results in a license or its equivalent, to practice any profession or occupation being denied, suspended, revoked, or otherwise acted against by a licensing authority in any jurisdiction.

(m) Being the subject of final agency action or its equivalent, issued by an appropriate regulator, for engaging in unlicensed activity as a money services business or deferred presentment provider in any jurisdiction.

(n) Committing any act resulting in a license or its equivalent to practice any profession or occupation being denied, suspended, revoked, or otherwise acted against by a licensing authority in any jurisdiction for a violation of 18 U.S.C. s. 1956, 18 U.S.C. s. 1957, 18 U.S.C. s. 1960, 31 U.S.C. s. 5324, or any other law or rule of another state or of the United States relating to a money services business, deferred presentment provider, or usury that may cause the denial, suspension, or revocation of a money services business or deferred presentment provider license or its equivalent in such jurisdiction.

(o) Having been convicted of, or entered a plea of guilty or nolo contendere to, any felony or crime punishable by imprisonment of 1 year or more under the law of any state or the United States which involves fraud, moral turpitude, or dishonest dealing, regardless of adjudication.

(p) Having been convicted of, or entered a plea of guilty or nolo contendere to, a crime under 18 U.S.C. s. 1956 or 31 U.S.C. s. 5318, s. 5322, or s. 5324, regardless of adjudication.

(q) Having been convicted of, or entered a plea of guilty or nolo contendere to, misappropriation, conversion, or unlawful withholding of moneys belonging to others, regardless of adjudication.

(r) Having been convicted of, or entered a plea of guilty or nolo contendere to, a violation of 31 C.F.R. chapter X, part 1022, regardless of adjudication.

(s) ~~(r)~~ Failure to inform the office in writing within 30 days after having pled guilty or nolo contendere to, or being convicted of, any felony or crime punishable by imprisonment of 1 year or more under the law of any state or the United States, or any crime involving fraud, moral turpitude, or dishonest dealing.

(t) ~~(s)~~ Aiding, assisting, procuring, advising, or abetting any person in violating a provision of this chapter or any order or rule of the office or commission.

(u) ~~(t)~~ Failure to pay any fee, charge, or cost imposed or assessed under this chapter.

(v) ~~(u)~~ Failing to pay a fine assessed by the office within 30 days after the due date as stated in a final order.

(w) ~~(v)~~ Failure to pay any judgment entered by any court within 30 days after the judgment becomes final.

(x) ~~(w)~~ Engaging or advertising engagement in the business of a money services business or deferred presentment provider without a license, unless exempted from licensure.

(y) ~~(x)~~ Payment to the office for a license or other fee, charge, cost, or fine with a check or electronic transmission of funds that is dishonored by the applicant's or licensee's financial institution.

(z) ~~(y)~~ Violations of 31 C.F.R. ss. 1010.306, 1010.311, 1010.312, 1010.340, 1010.410, 1010.415, 1022.210, 1022.320, 1022.380, and 1022.410, and United States Treasury Interpretive Release 2004-1.

(aa) ~~(z)~~ Any practice or conduct that creates the likelihood of a material loss, insolvency, or dissipation of assets of a money services business or otherwise materially prejudices the interests of its customers.

(bb) ~~(aa)~~ Failure of a check casher to maintain a federally insured depository account as required by s. 560.309.

(cc) ~~(bb)~~ Failure of a check casher to deposit into its own federally insured depository account any payment instrument cashed as required by s. 560.309.

(dd) ~~(cc)~~ Violating any provision of the Military Lending Act, 10 U.S.C. s. 987, or the regulations adopted under that act in 32 C.F.R. part 232, in connection with a deferred presentment transaction conducted under part IV of this chapter.

(ee) Failure to comply with the notification requirements in s. 501.171(3) and (4).

(2) ~~Pursuant to s. 120.60(6),~~ The office shall issue an emergency order suspending ~~may summarily suspend~~ the license of a money services business if the office finds that a licensee poses an immediate, serious danger to the public health, safety, and welfare. ~~A proceeding in which the office seeks the issuance of a final order for the summary suspension of a licensee shall be conducted by the commissioner of the office, or his or her designee, who shall issue such order.~~ The following acts are deemed by the Legislature to constitute an immediate and serious danger to the public health, safety, and welfare, and the office shall ~~may~~ immediately suspend the license of a money services business without making any further findings of immediate danger, necessity, and procedural fairness if:

(a) The money services business fails to provide to the office, upon written request, any of the records required by s. 560.123, s. 560.1235, s. 560.211, or s. 560.310 or any rule adopted under those sections. The suspension may be rescinded if the licensee submits the requested records to the office.

(b) The money services business fails to maintain a federally insured depository account as required by s. 560.208(4) or s. 560.309.

(c) A natural person required to be listed on the license application for a money services business pursuant to s. 560.141(1)(a)3. is criminally charged with, or arrested for, a crime described in paragraph (1)(o), paragraph (1)(p), or paragraph(1)(q).

Section 6. Section 560.1311, Florida Statutes, is created to read:

560.1311 Information security programs; cybersecurity event investigations.—

(1) DEFINITIONS.—As used in this section, the term:

(a) "Customer" means a person who seeks to obtain or who obtains or has obtained a financial product or service from a licensee.

(b) "Customer information" means any record containing nonpublic personal information about a customer of a financial transaction, whether on paper, electronic, or in other forms, which is handled or maintained by or on behalf of the licensee or its affiliates.

(c) "Cybersecurity event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

<u>(d) "Financial product or service" means any product or service offered by a licensee under this chapter.</u>

<u>(e) "Information security program" means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.</u>

<u>(f) "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 an industrial process control system, telephone switching and private branch exchange system, or environmental control system, which contain customer information or which are connected to a system that contains customer information.</u>

<u>(g)1. "Nonpublic personal information" means:</u>

<u>a. Personally identifiable financial information; and</u>

<u>b. Any list, description, or other grouping of customers that is derived using any personally identifiable financial information that is not publicly available, such as account numbers, including 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.</u>

<u>2. The term does not include:</u>

CODING: Words ~~stricken~~ are deletions; words <u>underlined</u> are additions.

a. Publicly available information, except as included on a list, description, or other grouping of customers described in sub-subparagraph 1.b.;

b. Any list, description, or other grouping of consumers, or any publicly available information pertaining to such list, description, or other grouping of consumers, which is derived without using any personally identifiable financial information that is not publicly available; or

c. 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 of the individuals on the list is a customer of a licensee.

3. As used in this paragraph, the term:

a.(I) "Personally identifiable financial information" means any information that:

(A) A customer provides to a licensee to obtain a financial product or service, such as information that a customer provides to a licensee on an application to obtain a loan or other financial product or service;

(B) A licensee receives about a consumer that is obtained during or as a result of any transaction involving a financial product or service between the licensee and the customer, such as information collected through an information-collecting device from a web server; or

(C) A licensee otherwise obtains about a customer in connection with providing a financial product or service to the customer, such as the fact that an individual is or has been one of the licensee's customers or has obtained a financial product or service from the licensee.

(II) The term "personally identifiable financial information" does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; or

(B) Information that does not identify a customer, such as blind data or aggregate information that does not contain personal identifiers such as account numbers, names, or addresses.

b.(I) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(A) Federal, state, or local government records, such as government real estate records or security interest filings;

(B) Widely distributed media, such as information from a telephone records repository or directory, a television or radio program, a newspaper, a social media platform, 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, so long as access is available to the general public; or

(C) Disclosures to the general public which are required to be made by federal, state, or local law.

(II) As used in this sub-subparagraph, the term "reasonable basis to believe is lawfully made available to the general public" relating to any information means that the person has taken steps to determine:

(A) That the information is of the type that is available to the general public, such as information included on the public record in the jurisdiction where the mortgage would be recorded; and

(B) Whether an individual can direct that the information not be made available to the general public and, if so, the customer to whom the information relates has not done so, such as when a telephone number is listed in a telephone directory and the customer has informed the licensee that the telephone number is not unlisted.

(h) "Third-party service provider" means a person, other than a licensee, which contracts with a licensee to maintain, process, or store nonpublic personal information, or is otherwise permitted access to nonpublic personal information through its provision of services to a licensee.

(2) INFORMATION SECURITY PROGRAM.—

(a) Each licensee shall develop, implement, and maintain a comprehensive written information security program that contains

<u>administrative, technical, and physical safeguards for the protection of the licensee's information system and nonpublic personal information.</u>

<u>(b) Each licensee shall ensure that the information security program meets all of the following criteria:</u>

<u>1. Be commensurate with the following measures:</u>

<u>a. Size and complexity of the licensee.</u>

<u>b. Nature and scope of the licensee's activities, including the licensee's use of third-party service providers.</u>

<u>c. Sensitivity of nonpublic personal information that is used by the licensee or that is in the licensee's possession, custody, or control.</u>

<u>2. Be designed to do all of the following:</u>

<u>a. Protect the security and confidentiality of nonpublic personal information and the security of the licensee's information system.</u>

<u>b. Protect against threats or hazards to the security or integrity of nonpublic personal information and the licensee's information system.</u>

<u>c. Protect against unauthorized access to or the use of nonpublic personal information and minimize the likelihood of harm to any customer.</u>

<u>3. Define and periodically reevaluate the retention schedule and the mechanism for the destruction of nonpublic personal information if retention is no longer necessary for the</u>

licensee's business operations or is no longer required by applicable law.

4. Regularly test and monitor systems and procedures for the detection of actual and attempted attacks on, or intrusions into, the licensee's information system.

5. Be monitored, evaluated, and adjusted, as necessary, to meet all of the following requirements:

a. Determine whether the licensee's information security program is consistent with relevant changes in technology.

b. Confirm the licensee's information security program accounts for the sensitivity of nonpublic personal information.

c. Identify changes that may be necessary to the licensee's information system.

d. Eliminate any internal or external threats to nonpublic personal information.

e. Amend the licensee's information security program for any of the licensee's changing business arrangements, including, but not limited to, mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements.

(c)1. As part of a licensee's information security program, the licensee shall establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises:

a. The confidentiality, integrity, or availability of nonpublic personal information in the licensee's possession;

b. The licensee's information system; or

c. The continuing functionality of any aspect of the licensee's operations.

2. The written incident response plan must address all of the following:

a. The licensee's internal process for responding to a cybersecurity event.

b. The goals of the licensee's incident response plan.

c. The assignment of clear roles, responsibilities, and levels of decisionmaking authority for the licensee's personnel that participate in the incident response plan.

d. External communications, internal communications, and information sharing related to a cybersecurity event.

e. The identification of remediation requirements for weaknesses identified in information systems and associated controls.

f. The documentation and reporting regarding cybersecurity events and related incident response activities.

g. The evaluation and revision of the incident response plan, as appropriate, following a cybersecurity event.

h. The process by which notice must be given as required under subsection (4) and s. 501.171(3) and (4).

(d)1. This section does not apply to a licensee that has fewer than:

a. Twenty individuals on its workforce, including employees and independent contractors; or

b. Five hundred customers during a calendar year.

2. A licensee that no longer qualifies for exemption under subparagraph 1. has 180 calendar days to comply with this section after the date of the disqualification.

(e) Each licensee shall maintain a copy of the information security program for a minimum of 5 years and shall make it available to the office upon request or as part of an examination.

(3) CYBERSECURITY EVENT INVESTIGATION.—

(a) If a licensee discovers that a cybersecurity event has occurred or that a cybersecurity event may have occurred, the licensee, or an outside vendor or third-party service provider that the licensee has designated to act on its behalf, shall conduct a prompt investigation of the cybersecurity event.

(b) During the investigation, the licensee, or the outside vendor or third-party service provider that the licensee has designated to act on its behalf, shall, at a minimum, determine as much of the following as possible:

1. Confirm that a cybersecurity event has occurred.

2. Identify the date that the cybersecurity event first occurred.

3. Assess the nature and scope of the cybersecurity event.

4. Identify all nonpublic personal information that may have been compromised by the cybersecurity event.

<u>5. Perform or oversee reasonable measures to restore the security of any compromised information system in order to prevent further unauthorized acquisition, release, or use of nonpublic personal information that is in the licensee's, outside vendor's, or third-party service provider's possession, custody, or control.</u>

<u>(c) If a licensee learns that a cybersecurity event has occurred, or may have occurred, in an information system maintained by a third-party service provider of the licensee, the licensee shall complete an investigation in compliance with this section or confirm and document that the third-party service provider has completed an investigation in compliance with this section.</u>

<u>(d) A licensee shall maintain all records and documentation related to the licensee's investigation of a cybersecurity event for a minimum of 5 years after the date of the cybersecurity event and shall produce the records and documentation to the office upon request.</u>

<u>(4) NOTICE TO OFFICE OF SECURITY BREACH.—</u>

<u>(a) Each licensee shall provide notice to the office of any breach of security affecting 500 or more individuals in this state at a time and in the manner prescribed by commission rule.</u>

<u>(b) Each licensee shall, upon the office's request, provide a quarterly update of a cybersecurity event investigation under subsection (3) until conclusion of the</u>

investigation.

(5) CONSTRUCTION.—This section may not be construed to relieve a covered entity from complying with s. 501.171. To the extent a licensee is a covered entity, as defined in s. 501.171(1), the licensee remains subject to s. 501.171.

(6) RULES.—The commission may adopt rules to administer this section, including rules that allow a licensee that is in full compliance with the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 C.F.R. part 314, to be deemed in compliance with subsection (2).

Section 7. Section 655.0171, Florida Statutes, is created to read:

655.0171 Requirements for customer data security and for notices of security breaches.—

(1) DEFINITIONS.—As used in this section, the term:

(a) "Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of a financial institution does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use. As used in this paragraph, the term "data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(b) "Department" means the Department of Legal Affairs.

(c)1. "Personal information" means:

a. An individual's first name, or first initial, and last name, in combination with any of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to the individual's financial account;

(IV) The individual's biometric data as defined in s. 501.702; or

(V) Any information regarding the individual's geolocation; or

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual which has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by

any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(2) REQUIREMENTS FOR DATA SECURITY.—Each financial institution shall take reasonable measures to protect and secure data that are in electronic form and that contain personal information.

(3) NOTICE TO OFFICE AND DEPARTMENT OF SECURITY BREACH.—

(a)1. Each financial institution shall provide notice to the office of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the office as expeditiously as practicable, but no later than 30 days after the determination of the breach or the determination of a reason to believe that a breach has occurred.

2. The written notice to the office must include the items required under s. 501.171(3)(b).

3. A financial institution must provide the following information to the office upon its request:

a. A police report, incident report, or computer forensics report.

b. A copy of the policies in place regarding breaches.

4. Steps that have been taken to rectify the breach.

5. A financial institution may provide the office with supplemental information regarding a breach at any time.

(b) Each financial institution shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department in accordance with s. 501.171.

(4) NOTICE TO INDIVIDUALS OF SECURITY BREACH.—Each financial institution shall give notice to each individual in this state whose personal information was, or the financial institution reasonably believes to have been, accessed as a result of the breach in accordance with s. 501.171(4). The notice must be provided no later than 30 days after the determination of the breach or the determination of a reason to believe that a breach has occurred. A financial institution may receive 15 additional days to provide notice to individuals of a security breach as required in this subsection if good cause for delay is provided in writing to the office within 30 days after determination of the breach or determination of the reason to believe that a breach has occurred.

(5) NOTICE TO CREDIT REPORTING AGENCIES.—If a financial institution discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the financial institution shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

Section 8. Paragraph (d) of subsection (1) of section

655.045, Florida Statutes, is amended to read:

655.045 Examinations, reports, and internal audits; penalty.—

(1) The office shall conduct an examination of the condition of each state financial institution at least every 18 months. The office may conduct more frequent examinations based upon the risk profile of the financial institution, prior examination results, or significant changes in the institution or its operations. The office may use continuous, phase, or other flexible scheduling examination methods for very large or complex state financial institutions and financial institutions owned or controlled by a multi-financial institution holding company. The office shall consider examination guidelines from federal regulatory agencies in order to facilitate, coordinate, and standardize examination processes.

(d) As used in this section, the term "costs" means the salary and travel expenses directly attributable to the field staff examining the state financial institution, subsidiary, or service corporation, and the travel expenses of any supervisory staff required as a result of examination findings. The mailing of any costs incurred under this subsection must be postmarked within 45 ~~30~~ days after the date of receipt of a notice stating that such costs are due. The office may levy a late payment of up to $100 per day or part thereof that a payment is overdue, unless excused for good cause. However, for intentional late payment of costs, the office may levy an administrative fine of up to $1,000 per day for each day the payment is overdue.

Section 9. Subsection (2) of section 657.005, Florida Statutes, is amended to read:

657.005 Application for authority to organize a credit union; investigation.—

(2) Any five or more individuals, a majority of whom are residents of this state and all of whom ~~who~~ represent a limited field of membership, may apply to the office for permission to organize a credit union. The fact that individuals within the proposed limited field of membership have credit union services available to them through another limited field of membership shall not preclude the granting of a certificate of authorization to engage in the business of a credit union.

Section 10. Subsection (1) of section 657.024, Florida Statutes, is amended to read:

657.024 Membership meetings.—

(1) The members shall receive timely notice of the annual meeting and any special meetings of the members, which shall be held at the time, place, and in the manner provided in the bylaws. The annual meeting and any special meetings of the members may be held virtually and without a quorum, subject to the bylaws.

Section 11. Subsections (6) and (7) of section 657.042, Florida Statutes, are renumbered as subsections (5) and (6), and

paragraph (b) of subsection (3) and present subsection (5) of that section are amended to read:

657.042 Investment powers and limitations.—A credit union may invest its funds subject to the following definitions, restrictions, and limitations:

(3) INVESTMENT SUBJECT TO LIMITATION OF TWO PERCENT OF CAPITAL OF THE CREDIT UNION.—

(b) Commercial paper and bonds of any corporation within the United States which have a fixed maturity, as provided in subsection (6) ~~(7)~~, except that the total investment in all such paper and bonds may not exceed 10 percent of the capital of the credit union.

~~(5) INVESTMENTS IN REAL ESTATE AND EQUIPMENT FOR THE CREDIT UNION.—~~

~~(a) Up to 5 percent of the capital of the credit union may be invested in real estate and improvements thereon, furniture, fixtures, and equipment utilized or to be utilized by the credit union for the transaction of business.~~

~~(b) The limitations provided by this subsection may be exceeded with the prior written approval of the office. The office shall grant such approval if it is satisfied that:~~

~~1. The proposed investment is necessary.~~

~~2. The amount thereof is commensurate with the size and needs of the credit union.~~

~~3. The investment will be beneficial to the members.~~

~~4. A reasonable plan is developed to reduce the investment to statutory limits.~~

Section 12. Paragraphs (b) and (c) of subsection (4) of section 658.21, Florida Statutes, are amended to read:

658.21 Approval of application; findings required.—The office shall approve the application if it finds that:

(4)

(b) At least two of the proposed directors who are not also proposed officers must have had within the 10 years before the date of the application at least 1 year of direct experience as an executive officer, regulator, or director of a financial institution as specified in the application ~~within the 5 years before the date of the application~~. ~~However, if the applicant demonstrates that at least one of the proposed directors has very substantial experience as an executive officer, director, or regulator of a financial institution more than 5 years before the date of the application, the office may modify the requirement and allow the applicant to have only one director who has direct financial institution experience within the last 5 years.~~

(c) The proposed president or chief executive officer must have had at least 1 year of direct experience as an executive officer, director, or regulator of a financial institution within the last 10 ~~5~~ years. In making a decision, the office must also consider ~~may waive this requirement after considering~~:

1. The adequacy of the overall experience and expertise of the proposed president or chief executive officer;

2. The likelihood of successful operation of the proposed state bank or trust company pursuant to subsection (1);

3. The adequacy of the proposed capitalization under subsection (2);

4. The proposed capital structure under subsection (3);

5. The experience of the other proposed officers and directors; and

6. Any other relevant data or information.

Section 13. Subsection (2) of section 658.33, Florida Statutes, is amended to read:

658.33 Directors, number, qualifications; officers.—

(2) Not less than a majority of the directors must, during their whole term of service, be citizens of the United States, and at least a majority of the directors must have resided in this state for at least 1 year preceding their election and must be residents therein during their continuance in office. In the case of a bank or trust company with total assets of less than $150 million, at least one, and in the case of a bank or trust company with total assets of $150 million or more, two of the directors who are not also officers of the bank or trust company must have had at least 1 year of direct experience as an executive officer, regulator, or director of a financial institution within the last <u>10</u> ~~5~~ years.

Section 14. Subsection (4) of section 662.141, Florida Statutes, is amended to read:

662.141 Examination, investigations, and fees.—The office may conduct an examination or investigation of a licensed family trust company at any time it deems necessary to determine whether the licensed family trust company or licensed family trust company-affiliated party thereof has violated or is about to violate any provision of this chapter, any applicable provision of the financial institutions codes, or any rule adopted by the commission pursuant to this chapter or the codes. The office may conduct an examination or investigation of a family trust company or foreign licensed family trust company at any time it deems necessary to determine whether the family trust company or foreign licensed family trust company has engaged in any act prohibited under s. 662.131 or s. 662.134 and, if a family trust company or a foreign licensed family trust company has engaged in such act, to determine whether any applicable provision of the financial institutions codes has been violated.

(4) For each examination of the books and records of a family trust company, licensed family trust company, or foreign licensed family trust company as authorized under this chapter, the trust company shall pay a fee for the costs of the examination by the office. As used in this section, the term "costs" means the salary and travel expenses of field staff

which are directly attributable to the examination of the trust company and the travel expenses of any supervisory and support staff required as a result of examination findings. The mailing of payment for costs incurred must be postmarked within 45 ~~30~~ days after the receipt of a notice stating that the costs are due. The office may levy a late payment of up to $100 per day or part thereof that a payment is overdue unless waived for good cause. However, if the late payment of costs is intentional, the office may levy an administrative fine of up to $1,000 per day for each day the payment is overdue.

Section 15. Subsection (21) of section 517.12, Florida Statutes, is amended to read:

517.12 Registration of dealers, associated persons, intermediaries, and investment advisers.—

(21) The registration requirements of this section do not apply to any general lines insurance agent or life insurance agent licensed under chapter 626, with regard to the sale of a security as defined in s. 517.021(34)(g) ~~s. 517.021(33)(g)~~, if the individual is directly authorized by the issuer to offer or sell the security on behalf of the issuer and the issuer is a federally chartered savings bank subject to regulation by the Federal Deposit Insurance Corporation. Actions under this subsection constitute activity under the insurance agent's license for purposes of ss. 626.611 and 626.621.

Section 16. This act shall take effect July 1, 2026.