The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Appropriations Committee on Agriculture, Environment, and General Government

BILL:	CS/SB 540
INTRODUCER:	Banking and Insurance Committee and Senator Martin
SUBJECT:	Office of Financial Regulation
DATE:	February 11, 2026
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Moody	Knudson	BI	**Fav/CS**
2.	Sanders	Betta	AEG	**Pre-meeting**
3.			RC	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 540 modifies the provisions of laws governing financial services regulated by the Office of Financial Regulation (OFR).

Cybersecurity

Mortgage brokers, mortgage lenders, and money services businesses

The bill:

- Creates a regulatory framework patterned after the Federal Standards for Safeguarding Customer Information ("Safeguard Rules") requiring mortgage brokers, mortgage lenders, and money services businesses licensees to create and maintain a written information security program that meets specified criteria and is designed for certain purposes.
- Requires licensees to:
  - Test, monitor, and adjust the program to meet specified requirements.
  - Establish a written incident response plan that consists of certain information.
  - Investigate any cybersecurity event which must determine specified information.
  - Maintain certain records for a specified time.
  - Notify the OFR of certain breaches of security.
  - Provide specified updates required by the OFR.
- Exempts certain licensees from the regulatory requirements established in the bill.

- Provides licensees are not exempt from complying with security requirements under consumer protection laws.
- Authorizes the Financial Services Commission (Commission) to adopt rules to administer provisions in this section of the bill.

The bill authorizes the OFR to impose disciplinary actions or penalties against the licensees for failing to comply with certain notice requirements.

Financial Institutions

The bill requires a financial institution to comply with security measures of personal information that are substantially similar to the security requirements under the consumer protection laws in ch. 501, F.S. A financial institution is required to comply with specified notice requirements to the Department of Legal Affairs (DLA), and certain individuals and consumer reporting agencies.

Securities Transactions

The bill amends the definition of "investment adviser" and the definition of "family office" to exclude certain persons and exempt certain offers or sales of securities from regulation and define the term "place of business."

Surrendered or Repossessed Vehicles

The bill provides that a parties' rights and obligations with respect to a surrendered or repossessed motor vehicle are exclusively governed by the Uniform Commercial Code, Secured Transactions, part VI of ch. 679, F.S.

Money Services Businesses Disciplinary Actions

The bill clarifies that an affiliated party of a money services business which is subject to disciplinary action and penalties must have been affiliated at the time the actionable grounds occurred and provides additional grounds for disciplinary action and penalties.

The bill requires, rather than authorizes, the OFR to issue an "emergency order" to suspend, instead of summarily suspending, the license of a money services business if the OFR makes certain findings. The bill clarifies that no further findings of immediate danger, necessity, or procedural fairness are required if certain facts exist.

Financial Institutions Director and Officer Qualifications

The bill allows certain directors and officers to have certain minimum experience within 10 years, rather than within five years of applying to form a banking corporation or trust company.

Credit Unions

The bill requires the majority of five or more individual applicants, rather than all individual applicants, that organize a credit union must be residents of the state. The bill allows credit union members to meet electronically and without an in-person quorum and allows virtual attendees to satisfy quorum requirements. The bill eliminates the limit on fixed asset investments.

Financial Institutions and Family Trust Companies Examination Costs

The bill requires that certain financial institutions and family trust companies must pay examination costs within 45 days, instead of within 30 days.

The bill does not impact state revenues and expenditures. See Section V., Fiscal Impact Statement.

The bill is effective July 1, 2026.

II. Present Situation:

The Office of Financial Regulation (OFR) is responsible for regulating all activities of banks, credit unions, other financial institutions, finance companies, and the securities industry (together, the "financial services").[1] The number of licensees or state-chartered institutions regulated by the OFR is summarized below:[2]

Division	Number of Persons Regulated
Division of Consumer Finance	122,530
Division of Financial Institutions	196
Division of Securities	403,627
Total Regulated Persons	526,353

Cybersecurity

There are federal standards for protecting customer information and Florida consumer protection laws for data security; however, there are no cybersecurity regulations under the financial services provisions. The Department of Legal Affairs (DLA) is responsible for enforcing such a violation and may disclose information to OFR relating to a covered entity's[3] violation of data security requirements of confidential personal information under consumer protection laws but the OFR has no regulatory authority to enforce any violation of the data security provisions in the consumer protection laws.[4]

[1] Section 20.121(3)(a)2., F.S.
[2] The Office of Financial Regulation (OFR), *Fast Facts 12th Edition* (Jan. 2025), https://www.flofr.gov/docs/default-source/documents/fast-facts.pdf (last visited Jan. 20, 2026) (hereinafter cited as "2025 OFR Fast Facts").
[3] Section 501.171(1)(b), F.S., defines "covered entity" as a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. The term also includes governmental entities with respect to certain notice requirements.
[4] Section 501.171(9)(a), F.S.

Federal Standards for Safeguarding Customer Information

Financial institutions[5] subject to the Federal Trade Commission's (FTC) jurisdiction are regulated under the Federal Standards for Safeguarding Customer Information (Safeguard Rules).[6] The Safeguard Rules do not apply to financial institutions that maintain customer information[7] for fewer than 5,000 customers.[8,9] Financial institutions subject to the Safeguard Rules are required to develop, implement, and maintain a comprehensive written information security program[10] that must be tailored to the size and complexity of the institution's system and activities, and must meet other specified criteria.[11]

The information security program must also include several elements, for instance:

- Designating a qualified individual to oversee and implement the program;
- Basing the system on a risk assessment that identifies certain factors;
- Testing and monitoring the system;
- Implementing specified safeguards to control the risks;
- Implementing certain policies and procedures;
- Overseeing service providers;
- Evaluating and adjusting the program following the testing and monitoring results;
- Establishing a written incident response plan;
- Complying with reporting requirements; and
- Notifying the FTC of a qualifying event in certain circumstances.[12]

---

[5] 16 C.F.R. 314.2 defines "financial institution" as any institution the business of which is engaging in activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

[6] 16 C.F.R. 314.1(b).

[7] 16 C.F.R. 314.2(d) defines "customer information" as any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a financial institution or a financial institution's affiliates. 16 C.F.R. 314.2(l) defines (1) "nonpublic personal information" as (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. (2) Nonpublic personal information does not include: (i) Publicly available information; or (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available. 16 C.F.R. 314.2(b)(1) defines "consumer" as an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

[8] 16 C.F.R. 314.2(c) defines "customer" as a consumer who has a customer relationship with a financial institution. 16 C.F.R. 314.2(e)(1) defines "customer relationship" as a continuing relationship between a consumer and a financial institution under which the financial institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. 16 C.F.R. 314.2(g)(1) defines "financial product or service" as 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 (12 U.S.C. 1843(k)).

[9] 16 C.F.R. 314.6.

[10] 16 C.F.R. 314.2(i) defines "information security program" as 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.

[11] 16 C.F.R. 314.3(a).

[12] 16 C.F.R. 314.4.

A financial institution must notify the FTC of a notification event[13] that involves information of at least 5,000 consumers.[14] Such notification must be made as soon as possible, but no later than 30 days after discovery of the event, on the FTC's website and must include specified information.[15]

Florida Security of Confidential Personal Information

Section 501.171, F.S., provides covered entities, governmental entities, and third-party agents are required to take reasonable measures to protect and secure electronic data containing personal information.[16,17] When the security of a data system is breached, a covered entity must provide notice to the DLA, affected individuals, and credit reporting agencies in certain circumstances.[18] A covered entity that fails to provide the required notices may face civil penalties.[19]

Notice to the Department of Legal Affairs

Covered entities must provide written notice of any breach of security that affects 500 or more Floridians to the DLA within 30 days after the determination of the breach or a reason to believe a breach occurred.[20] The notice may be delayed an additional 15 days for good cause, if certain

[13] 16 C.F.R. 314.2(m) defines "notification event" as acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered encrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition will be 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 such information.
[14] 16 C.F.R. 314.4(j)(1).
[15] *Id.* Providing the notice must include: (i) The name and contact information of the reporting financial information; (ii) A description of the types of information that were involved in the notification event; (iii) If the information is possible to determine, the date or date range of the notification event; (iv) The number of consumers affected or potentially affected by the notification event; (v) A general description of the notification event; and (vi) Whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official.
[16] Section 501.171(1)(g), F.S., defines: 1. "personal information" as a. An individual's first name or first initial and last name in combination with one of the following: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other number issued by a governmental entity 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 needed to permit access to the financial account; (IV) An individual's medical history, mental or physical condition, or medical treatment or diagnosis; (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer; (VI) An individual's biometric data; or (VII) Any information regarding an individual's geolocation. b. A user name or e-mail address, in combination with a password or security question and answer is also considered "personal information." 2. Information that is publicly available from a federal, state, or local governmental entity or information that is encrypted, secured, or modified by a method or technology that removes personally identifiable information is not considered "personal information." Section 501.702(4), F.S., defines "biometric data" as data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs; video or audio recordings or data generated from video or audio recordings; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.
[17] Section 501.171(2), F.S.
[18] Section 501.171(3) - (5), F.S.
[19] Section 501.171(9), F.S.
[20] Section 501.171(3)(a), F.S.

conditions are met.[21] The notice must include specified information.[22] A covered entity must also provide certain information upon request of the DLA,[23] and may provide any other information regarding the breach to the DLA at any time to supplement the required information.[24]

Notice to Individuals

A covered entity must provide notice to each individual in Florida whose personal information was, or is reasonably believed to have been, accessed as a result of a breach. Notice must be provided as quickly as possible, taking into account the time needed to determine the scope of the breach of security, to identify affected individuals, and to restore reasonable integrity of the data system that was breached. However, notice must be provided within 30 days of determination of the breach or reason to believe a breach occurred unless specified exceptions apply.[25] The notice must be sent to the individual's mailing address or e-mail address and must include specified information.[26]

This notice may be substituted in lieu of direct notice to the individual if the cost of providing notice will exceed $250,000, the number of affected individuals exceeds 500,000, or the covered entity does not have an e-mail address or mailing address for the affected individuals.[27] The substitute notice must include a conspicuous notice on the Internet website of the covered entity, if the entity maintains a website, and notice in print and broadcast media, including major media in urban and rural areas where the affected individuals reside.[28]

Notice to Credit Reporting Agencies

If a breach requires more than 1,000 individuals to be notified at a single time, the covered entity must also notify all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notices.[29]

---

[21] *Id.*
[22] Section 501.171(3)(b), F.S. (providing the information that must be included is: 1. A synopsis of the events surrounding the breach at the time the notice is provided; 2. The number of individuals in this state who were or potentially have been affected by the breach; 3. Any services related to the breach being offered or scheduled to be offered by the covered entity to individuals, without charge, and instructions as to how to use such services; 4. A copy of the notice sent to individuals affected or potentially affected by the breach or an explanation of other actions being taken, such as a delay in notification at the request of law enforcement, a determination that the breach was unlikely to cause harm, or notice provided in compliance with federal law; and 5. The name, address, telephone number, and e-mail address of the employee of the covered entity from whom additional information may be obtained about the breach).
[23] Section 501.171(3)(c), F.S. (providing the information that must be provided is: 1. A police report, incident report, or computer forensics report; 2. A copy of the policies in place regarding breaches; and 3. Any steps taken by the covered entity to rectify the breach).
[24] Section 501.171(3)(d), F.S.
[25] Section 501.171(4)(a), F.S.
[26] Section 501.171(4)(d) and (e), F.S. (providing the notice must include: 1. The date, estimated date, or estimated date range of the breach of security; 2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security; and 3. Information that the individual can use to contact the covered entity about the breach of security and the individual's personal information maintained by the covered entity).
[27] Section 501.171(4)(f), F.S.
[28] *Id.*
[29] Section 501.171(5), F.S.

Securities Transactions

Federal Regulation

The Securities and Exchange Commission (SEC) oversees federal securities laws[30] broadly aimed at protecting investors; maintaining fair, orderly, and efficient markets; and facilitating capital formation.[31]

The SEC has broad regulatory authority over significant parts of the securities industry, including investment advisers.[32] Investment advisers are required to register with the SEC unless an exception to registration applies.[33] Federal law provides that a family office is not considered an investment adviser,[34] and defines "family office" as a company that: [35]

- Has no clients other than family clients,[36] with one exception;[37]
- Is wholly owned by family clients and is exclusively controlled (directly or indirectly) by one or more family members and/or family entities; and
- Does not hold itself out to the public as an investment adviser.

Securities Act of 1933

Following the stock market crash of 1929, the Securities Act of 1933[38] (Act of 1933) was enacted to regulate the offers and sales of securities. The Act of 1933 requires every offer and sale of securities to be registered with the Securities and Exchange Commission (SEC), unless an exemption from registration is available. The Act of 1933 requires issuers to disclose financial and other significant information regarding securities offered for public sale and prohibits deceit, misrepresentations, and other kinds of fraud in the sale of securities. The Act of 1933 requires

[30] Section 15, Securities and Exchange Act of 1934.
[31] Securities and Exchange Commission, *Mission*, https://www.sec.gov/about/mission (last visited Jan. 29, 2026).
[32] 15 U.S.C. 80b-1.
[33] 15 U.S.C. 80b-3.
[34] 17 C.F.R. 275.202(a)(11)(G)-1(a).
[35] 17 C.F.R. 275.202(a)(11)(G)-1(b).
[36] 17 C.F.R. 275.202(a)(11)(G)-1(d)(4) defines "family client" as (i) Any family member; (ii) Any former family member; (iii) Any key employee; (iv) Certain former key employee; (v) Any non-profit organization, charitable foundation, charitable trust, or other charitable organization, in each case for which all the funding such foundation, trust or organization holds came exclusively from one or more other family clients; (vi) Any estate of a family member, former family member, key employee, or, subject to specified conditions, former key employee; (vii) Any irrevocable trust in which one or more other family clients are the only current beneficiaries; (viii) Any irrevocable trust funded exclusively by one or more other family clients in which other family clients and non-profit organization, charitable foundations, charitable trusts, or other charitable organizations are the only current beneficiaries; (ix) Any revocable trust of which one or more other family clients are the sole grantor; (x) Any trust of which: Each trustee or other person authorized to make decisions with respect to the trust is a key employee; and each settlor or other person who has contributed assets to the trust is a key employee or the key employee's current and/or former spouse or spousal equivalent who, at the time of contribution, holds a join,, community property, or other similar shared ownership interest with the key employee; or (xi) Any company wholly owned (directly or indirectly) exclusively by, and operated for the sole benefit of, one or more other family clients; provided that if any such entity is a pooled investment vehicle, it is excepted from the definition of "investment company" under the Investment Company Act of 1940.
[37] 17 C.F.R. 275.202(a)(11)(G)-1(b) (providing that if a person that is not a family client becomes a client of a family office as a result of the death of a family member or key employee or other involuntary transfer from a family member or key employee, that person shall be deemed to be a family client for purposes of this section for one year following the completion of the transfer of legal title to the assets resulting from the involuntary event).
[38] Public Law 73-22, as amended through P.L. 117-268, enacted December 23, 2022.

issuers to disclose information deemed relevant to investors as part of the mandatory SEC registration of the securities that those companies offer for sale to the public.[39]

Registered securities offerings, often called public offerings, are available to all types of investors and have more rigorous disclosure requirements. Initial public offerings (IPOs) provide an initial pathway for companies to raise unlimited capital from the general public through a registered offering. After its IPO, the company will be a public company with ongoing public reporting requirements.[40]

By contrast, securities offerings that are exempt from SEC registration are referred to as private offerings and are mainly available to more sophisticated investors. The SEC exempts certain small offerings from registration requirements to foster capital formation by lowering the cost of offering securities to the public.[41]

Florida Regulation of Securities

The federal securities acts expressly allow for concurrent state regulation under blue sky laws,[42] which are designed to protect investors against fraudulent sales practices and activities. Most state laws typically require companies making offerings of securities to register their offerings before they can be sold in a particular state, unless a specific state exemption is available. The laws also license brokerage firms, their brokers, and investment adviser representatives.[43]

The scope of the OFR's jurisdiction includes the regulation and registration of the offer and sale of securities in, to, or from Florida by firms, branch offices, and individuals associated with these firms in accordance with the ch. 517, F.S.[44] The Division of Securities (division) within the OFR is responsible for administering the Securities and Investor Protection Act (SaIP Act). The SaIP Act prohibits dealers, associated persons, and issuers from offering or selling securities in this state unless registered with the OFR or specifically exempted.[45] Additionally, all securities in Florida must be registered with the OFR unless they meet one of the exemptions in ss. 517.051 or 517.061, F.S., or are federally covered (i.e., under the exclusive jurisdiction of the SEC).

[39] *Id.*
[40] U.S. Securities and Exchange Commission (SEC), *What does it mean to be a public company?* https://www.sec.gov/education/capitalraising/building-blocks/what-does-it-mean-be-a-public-company (last visited Jan. 28, 2024).
[41] 17 C.F.R. s. 230.251.
[42] The term "blue sky" derives from the characterization of baseless and broad speculative investment schemes, which such laws targeted. Cornell Law School, Blue Sky Laws https://www.law.cornell.edu/wex/blue_sky_law#:~:text=In%20the%20early%201900s%2C%20decades,schemes%20which%20such%20laws%20targeted (last visited Jan. 28, 2024) (last visited Jan. 29, 2026).
[43] SEC, *Blue Sky Laws*, http://www.sec.gov/answers/bluesky.htm (last visited Jan. 29, 2026).
[44] Pursuant to s. 20.121(3), F.S. The jurisdiction of the OFR also includes state-chartered financial institutions and finance companies.
[45] Section 517.12, F.S.

Florida Motor Vehicle Sales Finance Laws

The Florida Motor Vehicle Retail Sales Finance Act[46] regulates sellers,[47] commonly referred to as auto dealers, who enter into retail installment contracts[48] with buyers[49] for the purchase or lease of a motor vehicle.[50] Except for certain businesses, such as banks or trust companies, sellers are required to obtain a license to operate in Florida.[51] A seller must submit an application, specified information, and a nonrefundable fee to the Office of Financial Regulation (OFR) to obtain the required license.[52]

Any person who willfully and intentionally violates any provision of s. 520.995, F.S., or engages in the business of a retail installment seller without a license is guilty of a misdemeanor of the first degree. Section 520.995, F.S., provides grounds for disciplinary action by the OFR when, for instance, there is failure to comply with any provision of ch. 520, F.S. Further, the OFR has authority to issue and serve upon any person a cease and desist order whenever such person is violating, has violated, or is about to violate any provision of ch. 520, F.S.,[53] or may impose an administrative fine not to exceed $1,000 for each violation that has occurred.[54]

Retail installment contracts must comply with several requirements and prohibitions, including, but not limited to, that the agreement must:

- Be in writing;[55]
- Contain a "Notice to the Buyer" which includes specified information;[56] and
- Contain other specified information, including the amount financed, finance charges, total amount of payments, total sale price, and payment details.[57]

Sellers must provide buyers with a separate written itemization of the amount financed.[58] Florida law contains several other provisions to protect the buyer, such as regulation on insurance rates,

[46] Sections 520.01-520.10, 520.12, 520.125, and 520.13, F.S.
[47] Section 520.02(11), F.S., defines "motor vehicle retail installment seller" or "seller" as a person engaged in the business of selling motor vehicles to retail buyers in retail installment transactions.
[48] "Retail installment contract" or "contract" is defined as an agreement, entered into in this state, pursuant to which the title to, or a lien upon the motor vehicle, which is the subject matter of a retail installment transaction, is retained or taken by a seller from a retail buyer as security, in whole or in part, for the buyer's obligation. The term includes a conditional sales contract and a contract for the bailment or leasing of a motor vehicle by which the bailee or lessee contracts to pay as compensation for its use a sum substantially equivalent to or in excess of its value and by which it is agreed that the bailee or lessee is bound to become, or for no further or a merely nominal consideration, has the option of becoming, the owner of the motor vehicle upon full compliance with the provisions of the contract. Section 520.02(17), F.S.
[49] "Retail buyer" or "buyer" is defined as a person who buys a motor vehicle from a seller not principally for the purpose of resale, and who executes a retail installment contract in connection therewith or a person who succeeds to the rights and obligations of such person.
[50] *See* Ch. 520, F.S.
[51] Section 520.03(1), F.S.
[52] *Id.*
[53] Section 520.994(3), F.S.
[54] Section 520.994(4), F.S.
[55] Section 520.07(1)(a), F.S.
[56] Section 520.07(1)(b), F.S.
[57] Section 520.07(2), F.S.
[58] Section 520.07(3), F.S.

refunds for unearned insurance premiums, limits on the amount of delinquency charges a holder[59] may charge, and restrictions on when a contract may be signed with blank spaces.[60]

In conjunction with entering into any new retail installment contract or contract for a loan, a seller, a sales finance company,[61] or a retail lessor,[62] and any assignee of such an entity, may offer an optional guaranteed asset protection product[63] ("GAP product") for a fee or otherwise.[64]

A seller or any other authorized entity may not require the buyer to purchase a GAP product as a condition for making the loan. In order to offer a GAP product, a seller or any other authorized entity must comply with the following:[65]

- The cost of any GAP product must not exceed the amount of the loan indebtedness.
- Any contract or agreement pertaining to a GAP product must be governed by s. 520.07, F.S., relating to requirements and prohibitions as to retail installment contracts.
- A GAP product must remain the obligation of any person that purchases or otherwise acquires the loan contract covering such product.
- An entity providing GAP products must provide readily understandable disclosures that explain in detail eligibility requirements, conditions, refunds, and exclusions. The disclosures must explain that the purchase of the GAP product is optional, and must meet certain criteria regarding the language contained in it.
- An entity must provide a copy of the executed contract for the GAP product to the buyer.
- An entity may not offer a contract for a GAP product that contains terms giving the entity the right to unilaterally modify the contract unless:
  - The modification is favorable to the buyer and is made without any additional charge; or
  - The buyer is notified of any proposed change and is provided a reasonable opportunity to cancel the contract without penalty before the change goes in effect.
- If a contract for a GAP product is terminated, the entity must refund to the buyer all unearned portions of the purchase price of the contract unless the contract provides otherwise. A customer who receives the benefit of the GAP product is not entitled to a refund. The buyer must notify the entity of the event terminating the contract and request a refund within 90 days after the terminating event. An entity may offer a buyer a nonrefundable contract for

[59] Section 520.02(8), F.S., provides that a "holder" of a retail installment contract means the retail seller of a motor vehicle retail installment contract or an assignee of such contract.
[60] Section 520.07, F.S.
[61] Section 520.02(19), F.S., defines "sales finance company" as a person engaged in the business of purchasing retail installment contracts from one or more sellers. The term includes, but is not limited to, a bank or trust company, if so engaged. The term does not include the pledge of an aggregate number of such contracts to secure a bona fide loan thereon.
[62] Section 521.003(8), F.S., defines "retail lessor" as a person who regularly engages in the business of selling or leasing motor vehicles and who offers or arranges a lease agreement for a motor vehicle. The term includes an agent or affiliate who acts on behalf of the retail lessor and excludes any assignee of the lease agreement.
[63] Section 520.02(7), F.S., defines "guaranteed asset protection product" as a loan, lease, or retail installment contract term, or modification or addendum to a loan, lease, or retail installment contract, under which a creditor agrees, with or without a separate charge, to cancel or waive a customer's liability for payment of some or all of the amount by which the debt exceeds the value of the collateral that has incurred total physical damage or is the subject of an unrecovered theft. A guaranteed asset protection product may also provide, with or without a separate charge, a benefit that waives a portion of, or provides a customer with a credit toward, the purchase of a replacement motor vehicle. Such a product is not insurance for purposes of the Florida Insurance Code. This subsection also applies to all guaranteed asset protection products issued before October 1, 2008.
[64] Section 520.07(11), F.S.
[65] *Id.*

a GAP product only if the entity also offers the buyer a bona fide option to purchase a comparable contract that provides for a refund. Florida law prohibits an entity from deducting more than $75 in administrative fees from a refund.

- GAP products may be cancelable or non-cancelable after a free-look period.[66]
- If a GAP product is terminated because of:
  - A default under the retail installment contract or contract for a loan,
  - The repossession of the motor vehicle associated with such contract or loan, or
  - Any other termination of such contract or loan, a refund of the GAP product amount may be used to satisfy any balance owed on the retail installment contract or contract for a loan unless the buyer can show that the retail installment contract has been paid in full.

Money Services Businesses

The Office of Financial Regulation (OFR) regulates money services businesses (MSB) under ch. 560, F.S. A "money service business" is defined as any person located in or doing business in this state, from this state, or into this state from locations outside this state or country who acts as a payment instrument seller, foreign currency exchanger, check casher, or money transmitter. [67] The OFR is responsible for enforcing regulations and imposing disciplinary actions against MSBs.[68]

The OFR has authority to implement several disciplinary actions against a MSB for specified actions, such as failing to comply with the provisions of ch. 560, F.S., certain fraud or misrepresentation conduct, and refusing to allow the examination or inspection of books or files.[69] Section 560.114, F.S., provides for the following disciplinary actions:

- Issuing a cease and desist order;
- Issuing a removal order; or
- Denying, suspending, or revoking a license.[70]

Financial Institutions

A financial institution must have a federal or state charter to accept deposits. Banks are chartered and regulated as national banks by the Office of the Comptroller of the Currency (OCC) within the U.S. Department of the Treasury or as state banks by a state regulator.[71] The Florida Financial Institutions Codes apply to all state-authorized or state-chartered financial banks, trust

[66] Section 520.135(5), F.S., defines "free-look period" as the period of time, commencing on the effective date of the contract, during which the buyer may cancel the contract for a full refund of the purchase price. This period may not be shorter than 30 days.
[67] Section 560.103(23), F.S.
[68] Section 560.114(1), F.S.
[69] *Id.*
[70] *Id.*
[71] Congressional Research Service, In Focus, *Introduction to Financial Services: Banking*, p. 1, (Updated April 1 , 2025), https://www.congress.gov/crs-product/IF10035?q=%7B%22search%22%3A%22introduction+to+financial+services%3A++banking%22%7D&s=2&r=1 (last visited Jan. 29, 2026).

companies, and related entities.[72] Of the 196 financial entities regulated by the OFR, 57 of them are state-chartered banks.[73] There are also approximately 30 federally-chartered banks operating in Florida.[74]

Laws Relating to Directors and Executive Officers

Federally-chartered banks, publicly or privately held, must comply with rigorous regulatory requirements to become chartered.[75] No person is allowed to offer any national bank issued security unless certain registration requirements are filed with the OCC,[76] unless an exemption applies, such as nonpublic offerings.[77] State laws also specify requirements that a proposed new bank or trust company must comply with to be chartered, including minimum qualifications of directors and certain proposed executive officers.[78]

Initial Application

The OFR is required to make certain findings before approving an application to organize a bank or trust company.[79] One such finding is that the proposed directors and officers have sufficient financial institution experience, ability, standing, and reputation to indicate a reasonable promise of successful operation.[80] Specifically, the OFR must find that at least two of the proposed directors who are not also proposed officers, and the proposed president or proposed chief executive officer, have had at least one year of direct experience as an executive officer, regulator, or director of a financial institution within five years before the date of the application.[81] The OFR has authority to waive this experience requirement for the proposed president or chief executive officer after considering the following criteria:[82]

- The adequacy of the overall experience and expertise of the proposed president or chief executive officer;
- The likelihood of successful operation of the proposed state bank or trust company;
- The adequacy of the proposed capitalization;
- The proposed capital structure;
- The experience of the other proposed officers and directors; and
- Any other relevant data or information.

[72] Section 655.005(1)(k), F.S., states that the Financial Institutions Codes includes: Ch. 655, financial institutions generally; Ch. 657, credit unions; Ch. 658, banks and trust companies; Ch. 660, trust business; Ch. 662, family trust companies; Ch. 663, international banking; Ch. 665, relating to associations; and Ch. 667, savings banks.
[73] 2025 OFR Fast Facts.
[74] The OCC, *National Banks Active As of 11/30/2025*, November 30, 2025, national-by-state.pdf last visited Jan. 29, 2026).
[75] *See* 12 CFR 16; Office of the Comptroller of the Currency, *Comptroller's Licensing Manual Charters*, p. 4, December 2021, https://www.occ.gov/publications-and-resources/publications/comptrollers-licensing-manual/files/charters.pdf (last visited Jan. 29, 2026).
[76] 12 CFR 16.3
[77] 12 CFR 16.7
[78] Section 658.21, F.S.
[79] Section 658.21, F.S.
[80] Section 658.21(4)(a), F.S.
[81] Section 658.21(4)(b) and (c), F.S.
[82] Section 658.21(4)(c), F.S.

Director Qualifications

The board of directors of a bank or trust company must consist of at least five directors. Each director must be elected, except in cases when a director is appointed to fill a vacancy.[83] A majority of the directors must be United States citizens during their whole term of service, and must have resided in Florida for at least one year preceding their election, and must remain residents during their time in office.[84] 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 one year of direct experience as an executive officer, regulator, or director of a financial institution within the last five years.[85]

Disapproval of Directors and Executive Officers

Although federal law does not require a minimum amount of experience for proposed directors or executive officers, the appropriate Federal banking agency must issue a notice of disapproval if the competence, experience, character, or integrity of an individual indicates that it would not be in the best interests of the depositors of the depository institution or the public to permit the individual to be a director or be employed as a senior executive officer of the institution.[86] If the appropriate Federal banking agency issues a notice of disapproval before the end of a specified notice period, the entity may not add the individual to the board of directors.[87]

Similar to Federal law, Florida law also authorizes the OFR to disapprove the proposed appointment of any individual to the board of directors or employment of an individual as an executive officer if certain criteria are met, including, but not limited to, when the institution is non-compliant with minimum capital requirements or is otherwise operating in an unsafe and unsound condition.[88]

Credit Unions

A credit union must have a federal or state charter to operate in Florida. Credit unions are chartered and regulated as a national credit union by the National Credit Union Association (NCUA).[89] Such membership is limited to a group or groups with a common bond of occupation or association within a defined community. Deposits into a federal credit union allow members

[83] Section 658.33(1), F.S.
[84] Section 658.33(2), F.S.
[85] *Id.*
[86] 12 U.S.C. § 1831i(e).
[87] 12 U.S.C. § 1831i(b).
[88] Section 655.005(y), F.S., defines "unsafe and unsound practice" as: 1. any practice or conduct found by the office to be contrary to generally accepted standards applicable to a financial institution, or a violation of any prior agreement in writing or order of a state or federal regulatory agency, which practice, conduct, or violation creates the likelihood of loss, insolvency, or dissipation of assets or otherwise prejudices the interest of the financial institution or its depositors or members.
[89] National Credit Union Administration, *Overview of the Charter Application Process*, April 14, 2022, *https://ncua.gov/regulation-supervision/manuals-guides/federal-credit-union-charter-application-guide/overview-charter-application-process* (last visited Jan. 29, 2026).

to become owners of the credit union, run to become a credit union official, and vote on certain matters.[90]

The Florida Financial Institutions Codes apply to all state-chartered credit unions.[91] There are approximately 138 credit unions in Florida[92] with 67 of them being state-chartered.[93] Florida law provides that any person may be admitted to a credit union upon payment of any required fee, payment of shares, and compliance with the credit union bylaws.[94] State-chartered credit unions operate as financial institutions except for exercising certain incidental powers authorized by law.[95]

Member Qualifications

An application must be filed with the OFR to organize a credit union.[96] Any five or more residents of Florida who represent a limited field of membership may apply for permission to organize a credit union.[97] The application must be submitted on a prescribed form with specified information and a nonrefundable filing fee.[98]

Membership Meetings

Members are required to notice and hold the annual meeting and any special meetings of the members at the time, place, and in the manner provided in the bylaws. [99] Each member has one vote.[100] The members must elect the board of directors and other committees prescribed in the bylaws and transact any other business that the bylaws allow.[101]

Investments

Florida law regulates how credit unions may invest funds. There are no limits with respect to investing in some assets, for instance United States Treasury bonds. Examples of other classes of assets that are subject to investment limits include up to: [102]

- Twenty-five percent of the credit union's capital in shares or deposit accounts in any one corporate credit union or other insured financial depository institution.
- One percent of the credit union's capital in corporate obligations of any one corporation which is an affiliate or subsidiary of the credit union in certain circumstances.
- Five percent of the credit union's capital in real estate and improvements, furniture, fixtures, and equipment utilized by the credit union for the transaction of business. Credit unions may

[90] National Credit Union Administration, *Overview of Federal Credit Unions*, April 14, 2022, https://ncua.gov/regulation-supervision/manuals-guides/federal-credit-union-charter-application-guide/overview-federal-credit-unions (last visited Jan. 29, 2026).
[91] Section 655.005(1)(k), F.S., states that the Financial Institutions Codes includes ch. 657, credit unions.
[92] National Credit Union Service Organization, *Florida Credit Unions*, Florida Credit Unions (last visited Jan. 29, 2026).
[93] 2025 OFR Fast Facts at p. 4.
[94] Section 657.023(1), F.S.
[95] Section 657.031(3), F.S.
[96] Section 657.005(1), F.S.
[97] Section 657.005(2), F.S.
[98] Section 657.005(3), F.S.
[99] Section 657.024(1), F.S.
[100] Section 657.024(2), F.S.
[101] Section 657.024(4), F.S.
[102] Section 657.042, F.S.

receive prior written approval from the OFR to exceed the five percent limit if the following criteria is met:
- The proposed investment is necessary.
- The amount is commensurate with the size and needs of the credit union.
- The investment will be beneficial to the members.
- A reasonable plan is developed to reduce the investment to statutory limits.

In 2015, the NCUA removed the federal regulation that restricted federal credit unions from investing more than five percent aggregate in fixed-asset investments.[103]

Examination Costs

Financial Institutions

The OFR is required to conduct examinations of each financial institution at least once every 18 months. The OFR has discretion on whether to conduct more frequent examinations based upon the financial institution's risk profile, prior examination results, or significant changes in the institution or its operations.[104] The OFR may rely upon an examination conducted by an appropriate federal regulatory agency or may conduct a joint examination with the federal agency.[105] The OFR may conduct an examination or investigation of an affiliate[106] if the OFR has reason to believe that the conduct or business operations of such affiliate may have a negative impact on the state financial institution.[107]

The OFR may recover costs[108] of examination and supervision of a state financial institution, subsidiary, or service corporation that is engaged in an unsafe or unsound practice. The OFR may also recover costs of an authorized examination or investigation of an affiliate. Any costs a financial institution pays by mail must be postmarked within 30 days after the date of receipt of the notice stating that such costs are due. [109]

Family Trust Companies

The OFR may conduct an examination or investigation of a licensed family trust company to determine whether such company has violated or is about to violate any provision of ch. 662, F.S., any applicable provision of the Financial Institutions Code, or any rule adopted by the commission.[110] The OFR may also conduct an examination or investigation of a family trust company or foreign licensed family trust company to determine whether any applicable

[103] The NCUA, *Fixed-Asset Rule Provides Relief to More than 3,800 Federal Credit Unions*, July 2015, Fixed-Asset Rule Provides Relief to More than 3,800 Federal Credit Unions | NCUA (last visited Jan. 29, 2026).
[104] Section 655.045(1), F.S.
[105] Section 655.045(1)(a), F.S.
[106] Section 655.005(1)(a), F.S., defines "affiliate" as a holding company of a financial institution established pursuant to state or federal law, a subsidiary or service corporation of such holding company, or a subsidiary or service corporation of a financial institution.
[107] Section 655.045(1)(b), F.S.
[108] Section 655.045(1)(d), F.S., defines "costs" as 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.
[109] Section 655.045(1)(c), F.S.
[110] Section 662.141, F.S.

provisions of the Financial Institutions Code has been violated or whether such company has engaged in any of the following conduct:[111]

- Engaged in commercial banking;
- Engaged in unlicensed fiduciary services with the public;
- Served as personal representative or a copersonal representative of a probate estate;
- Served as an attorney in fact or agent;[112] or
- Advertised its services to the public.[113]

A family trust company, licensed family trust company, or foreign licensed family trust company must pay a fee for the costs[114] of the examinations conducted by the OFR. Any costs mailed by a trust company must be postmarked within 30 days after the receipt of a notice stating that the costs are due.[115]

III. Effect of Proposed Changes:

CS/SB 540, an act relating to the Office of Financial Regulation (OFR), modifies provisions of laws governing financial services regulated by OFR.

Cybersecurity

The bill creates three new sections relating to information security programs and cybersecurity event investigations. **Sections 1 and 7** of the bill subject: (a) mortgage brokers and lenders, and (b) money services businesses, to such cybersecurity regulation that are patterned after the Federal Safeguard Rules. **Section 8** subjects financial institutions to security requirements that are similar to the security requirements under consumer protection laws.

Mortgage Brokers and Lenders, and Money Services Businesses

Sections 1 and 7 of the bill regulate information security programs and cybersecurity event investigations of mortgage brokers and lenders, and money services businesses (MSB).

Information Security Program Requirements

Each licensee must 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. Each licensee must ensure that the information security program meets all of the following criteria:

- Be commensurate with the following measures:
  - Size and complexity of the licensee.
  - Nature and scope of the licensee's activities.

[111] *Id.*
[112] Section 662.131, F.S.
[113] Section 662.134, F.S.
[114] Section 662.141(4), F.S., defines "costs" as 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 the examination findings.
[115] *Id.*

  - Sensitivity of nonpublic personal information that is used by the licensee or that is in the licensee's possession, custody, or control.
- Be designed to do all of the following:
  - Protect the security and confidentiality of nonpublic personal information and the security of the licensee's information system.
  - Protect against threats or hazards to the security or integrity of nonpublic personal information and the licensee's information system.
  - Protect against unauthorized access to or the use of nonpublic personal information and minimize the likelihood of harm to any customer.
- 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 required by law.
- Regularly test and monitor systems and procedures for the detection of actual and attempted attacks on, or intrusions into, the licensee's information system.
- Be monitored, evaluated, and adjusted to meet the following requirements:
  - Determine whether the licensee's program is consistent with relevant changes in technology.
  - Confirm the licensee's program accounts for the sensitivity of nonpublic personal information.
  - Identify changes that may be necessary to the licensee's information system.
  - Eliminate any internal or external threats to nonpublic personal information.
  - Amend the licensee's program for any of the licensee's changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements.

The licensee must establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that includes:
- The confidentiality, integrity, or availability of nonpublic personal information in the licensee's possession;
- The licensee's information system; or
- The continuing functionality of any aspect of the licensee's operations.

The written incident response plan must address all of the following:
- The licensee's internal process for responding to a cybersecurity event.
- The licensee's incident response plan goals.
- The assignment of clear roles, responsibilities, and levels of decision making authority for the licensee's personnel that participate in the incident response plan.
- External communications, internal communications, and information sharing related to a cybersecurity event.
- The identification of remediation requirements for weaknesses identified in information systems and associated controls.
- The documentation and reporting regarding cybersecurity events and related incident response activities.
- The evaluation and revision of the incident response plan following a cybersecurity event.
- The process by which any required notice must be given.

A licensee that has fewer than:

- Twenty employees or independent contractors on its workforce; or
- Five hundred customers during a calendar year are not subject to the information technology program and cybersecurity event investigation requirements created in the bill. A licensee that no longer qualifies for such an exemption has 180 calendar days to comply with the requirements after the date of the disqualification. Each licensee shall maintain a copy of the information security program for a minimum of five years and must make it available to the office upon request or as part of an examination.

Cybersecurity Event Investigations

A licensee, or an outside vendor or third-party service provider that the licensee has designated to act on its behalf, must conduct a prompt investigation of the cybersecurity event if a cybersecurity event has or may have occurred. During the investigation, the licensee or outside vendor or third-party service provider must, to the extent possible comply with the following minimum requirements:

- Confirm that a cybersecurity event has occurred.
- Identify the date that the event first occurred.
- Assess the nature and scope of the cybersecurity event.
- Identify all nonpublic personal information that may have been compromised.
- 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.

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 must complete an investigation or confirm and document that the third-party service provider has completed an investigation that complies with the requirements provided in the bill and summarized above. A licensee must maintain all records and documentation related to the licensee's investigation of a cybersecurity event for a minimum of five years and must produce the records and documentation to the OFR upon request.

Notice of Security Breach

Each licensee must provide notice as prescribed by commission rule to the OFR of any security breach affecting 500 or more individuals. Upon the OFR's request, each licensee must provide a quarterly update of a cybersecurity event investigation until conclusion of the investigation.

Construction

The bill provides that covered entities are not relieved from complying with s. 501.171, F.S., and any licensee that is a covered entity under that chapter remains subject to the requirements of that section.

Rules

The bill authorizes the commission to adopt rules to administer the sections, including rules that allow a licensee that is in full compliance with the Safeguard Rules to be deemed in compliance with information security program requirements.

Definitions

The bill defines all of the following terms:

- "Customer" means a person who seeks to obtain or who obtains or has obtained a financial product or service from a licensee.
- "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.
- "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.
- "Financial product or service" means any product or service offered by a licensee.
- "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.
- "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.
- "Licensee" means a person licensed under the relevant chapter 494 or 560, F.S.
- "Nonpublic personal information" means:
    - Personally identifiable financial information;[116] and
    - Any list, description, or other grouping of customers which 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 which is derived, in whole or in part, using personally identifiable financial information that is not publicly available.
    - The term does not include:
    - Publicly available information,[117] except as included on a list, description, or other grouping of customers described above;

[116] "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 which 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. 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.

[117] "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

  - 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
  - Any list of individuals' names and addresses which contain 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.
- "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.

Financial Institutions

Section 8 of the bill requires each financial institution to take reasonable measures to protect and secure data that are in electronic form and that contain personal information.

Required Notices

Each financial institution must provide notice that meet specified requirements of any security breach affecting 500 or more individuals in Florida to all of the following entities or individuals:

- The OFR as expeditiously as practicable, but no later than 30 days after a determination that a breach has occurred or a reason to believe that a breach has occurred which must include all requirements under s. 501.171(3)(b), F.S., [118] and must include all of the following items:[119]
  - Upon request, provide the following information:
  - A police report, incident report, or computer forensics report.
  - A copy of the policies in place regarding breaches.
  - Steps that have been taken to rectify the breach.

---

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. 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.

[118] Section 501.171(3)(b), F.S. (requiring the following information to be provided in the written notice to the DLA: 1. A synopsis of the events surrounding the breach; 2. The number of individuals in the state who were or potentially have been affected by the breach; 3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions how to use such services; 4. A copy of the notice required to be provided to individuals or an explanation of the other actions taken regarding such notice; 5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach).

[119] A financial institution may provide the OFR with supplemental information at any time.

- The Department of Legal Affairs (DLA) in accordance with notice requirements of any security breach under consumer protection laws.[120]
- 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 the notice requirements of any security breach under consumer protection laws.[121] Such 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. This deadline may be extended for an additional 15 days if good cause for delay is provided in writing to the OFR within 30 days after determination of the breach or the reason to believe that a breach has occurred.
- If a financial institution discovers circumstances requiring notice to 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 a nationwide basis[122] of the timing, distribution, and content of the notices.

Definitions

- "Breach of security" or "breach" means unauthorized access of data in electronic form[123] 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.
- "Department" means the Department of Legal Affairs.
- "Personal information" means:
  - An individual's first name, or first initial, and last name, in combination with any of the following data for that individual:
    - A social security number;
    - A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document;
  - 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;
    - The individual's biometric data;[124] or
    - Any information regarding the individual's geolocation; or
  - A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.
  - The term does not include:

[120] *See* s. 501.171(3), F.S.
[121] *See* s. 501.171(4), F.S.
[122] 15 U.S.C. s. 1681a(p) defines "consumer reporting agency that complies and maintains files on consumers on a nationwide basis" as a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: (1) public record information. (2) Credit account information from persons who furnish that information regularly and in the ordinary course of business.
[123] 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.
[124] *Supra* note 16.

- Information about an individual which has been made publicly available by a federal, state, or local governmental entity.
- 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.

Disciplinary Actions and Penalties

Section 2 of the bill subjects mortgage brokers and mortgage lenders who are covered under the cybersecurity regulation to any administrative fines or penalties provided in s. 494.00255, F.S., for failure to comply with notification requirements to the DLA and individuals whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.[125] **Section 6** of the bill subjects money services businesses who are covered under the cybersecurity regulation to any disciplinary actions or penalties provided in s. 560.114, F.S., for failing to make such notifications.

Securities Transactions

Section 3 of the bill amends the definition of "investment adviser" to exclude the following persons from regulation as investment advisers:

- During the preceding 12 months, a person that:
  - Without a place of business in the state, has had fewer than six clients who are residents of the state.
  - With a place of business in the state, has had fewer than six clients who are residents of the state and no clients who are not residents of the state.

Current law provides a person that, during the preceding 12 months, has fewer than six clients who are residents of Florida are not investment advisers without distinguishing whether the place of business is in the state. Therefore, the amendment in the bill narrows the exemption in current law to provide that a person who has a place of business in Florida is not an investment adviser only if such business has no clients who are residents out-of-state during the preceding 12 months.

- A family office as defined by specified provisions in Securities and Exchange Commission Rule under the Investment Advisers Act of 1940, as amended.[126] The bill clarifies when determining whether a person meets the definition of "family offices," the following terms have the same meaning as in Securities and Exchange Commission Rule 202(a)(11)(G)-1(d), 17 C.F.R. s. 275.202(a)(11)(G)-1(d):
  - Affiliated family office;[127]
  - Control;[128]

[125] *See* s. 501.171(3) and (4), F.S.
[126] *Supra* 35; 17 C.F.R. s. 275.202(a)(11)(G)-1(b).
[127] 17 C.F.R. s. 275.202(a)(11)(G)-1(d)(1) defines "affiliated family office" as a family office wholly owned by family clients of another family office and that is controlled (directly or indirectly) by one or more family members of such other family office and/or family entities affiliated with such other family office and has no clients other than family clients of such other family office.
[128] 17 C.F.R. s. 275.202(a)(11)(G)-1(d)(2) defines "control" as the power to exercise a controlling influence over the management or policies of a company, unless such power is solely the result of being an officer of such company.

- Executive officer;[129]
- Family client;[130]
- Family entity;[131]
- Family member;[132]
- Former family member;[133]
- Key employee;[134] and
- Spousal equivalent.[135]

Section 4 of the bill provides the same definitions for these terms to clarify when an offer or sale of securities to a "family office" is exempt from registration requirements. Cross-references to the Securities and Exchange Commission Rule that defines "family office" are updated.

Section 3 of the bill also defines "place of business" as an office at which the investment adviser regularly provides investment advisory services to, 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 to, solicits, meets with, or otherwise communicates with clients.

Surrendered or Repossessed Motor Vehicles

Section 5 of the bill provides that a parties' rights and obligations with respect to a surrendered or repossessed motor vehicle are exclusively governed by the Uniform Commercial Code, Secured Transactions, part VI of ch. 679, F.S.

---

[129] 17 C.F.R. s. 275.202(a)(11)(G)-1(3) defines "executive officer" as the president, any vice president in charge of a principal business unit, division or function (such as administration or finance), any other officer who performs a policy-making function, or any other person who performs similar policy-making functions, for the family office.
[130] *Supra* 36.
[131][131] 17 C.F.R. s. 275.202(a)(11)(G)-1(5) defines "family entity" as any of the trusts, estates, companies or other entities described in the definition of "family client" in 17 C.F.R. s. 275.202(a)(11)(G)-1(d)(4)(v)-(ix) or (xi), but excluding key employees and their trusts from the definition of family client solely for purposes of this definition.
[132] 17 C.F.R. s. 275.202(a)(11)(G)-1(6) defines "family member" as all lineal descendants (including by adoption, stepchildren, foster children, and individuals that were a minor when another family member became a legal guardian of that individual) of a common ancestor (who may be living or deceased), and such lineal descendants' spouses or spousal equivalents; provided that the common ancestor is no more than 10 generations removed from the youngest generation of family members.
[133] 17 C.F.R. s. 275.202(a)(11)(G)-1(7) defines "former family member" as a spouse, spousal equivalent, or stepchild that was a family member but is no longer a family member due to a divorce or other similar event.
[134][134] 17 C.F.R. s. 275.202(a)(11)(G)-1(8) defines "key employee" as any natural person (including any key employee's spouse or spouse equivalent who holds a joint, community property, or other similar shared ownership interest with that key employee) who is an executive officer, director, trustee, general partner, or person serving in a similar capacity of the family office or its affiliated family office or any employee of the family office or its affiliated family office (other than an employee performing solely clerical, secretarial, or administrative functions with regard to the family office) who, in connection with his or her regular functions or duties, participates in the investment activities of the family office or affiliated family office, provided that such employee has been performing such functions and duties for or on behalf of the family office or affiliated family office, or substantially similar functions or duties for or on behalf of another company, for at least 12 months.
[135] 17 C.F.R. s. 275.202(a)(11)(G)-1(9) defines "spousal equivalent" as cohabitant occupying a relationship generally equivalent to that of a spouse.

Money Services Businesses Disciplinary Actions and Penalties

Grounds for Disciplinary Actions and Penalties

Section 6 of the bill clarifies that an affiliated of a money services business that is subject to disciplinary actions and penalties of ch. 560, F.S., must be affiliated at the time of commission of the actions. Grounds for disciplinary actions and penalties are expanded to include being convicted, or entering a plea to a crime, regardless of adjudication, to the following provisions:

- A violation of the 31 U.S.C., Bank Secrecy Act, relating to:
  - Section 5318 requiring appropriate procedures and reporting requirements to guard against money laundering, the financing of terrorism, or other forms of illicit finance; compliance with lawful summons; and reporting suspicious transactions.
  - Section 5322 providing for criminal penalties relating to the following provisions or rules prescribed under such sections:
    - 31 USC Subtitle IV, Chapter 53, Subchapter II (except ss. 5315, 5324, and 5336), relating to records and reports on money instruments transactions or an order issued under such subchapter.
    - Section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91-508, relating to retention of records and compliance with such retention requirements by depository institutions.
    - 31 U.S.C. s. 5318(a)(2) relating to a domestic financial institutions obligation to maintain appropriate procedures to ensure compliance with anti-money laundering regulations.
    - 31 U.S.C. s. 5318(i) relating to certain financial institution's requirements to maintain due diligence policies and procedures.
    - 31 U.S.C. s. 5318(j) relating to prohibitions on United States Correspondent Accounts with Foreign Shell Banks.
    - 31 U.S.C. s. 5318A relating to special measures required by the Secretary of Treasury.
- A violation of 31 C.F.R. ch. X, part 1022, relating to rules for anti-money laundering programs for money services businesses, including requirements to establish policies and procedures for such program, and comply with reporting and filing provisions.

Orders Suspending a License

The bill requires, rather than authorizes, the OFR to issue an emergency order suspending, rather than summarily suspending, a money services business license when the OFR finds that a licensee poses an immediate, serious danger to the public health, safety, and welfare. A corresponding provision related to the OFR seeking a final order for the summary suspension is removed because the provision is no longer relevant.

No further findings of immediate danger, necessity, and procedural fairness are required before ordering the suspension in specified situations. One such situation applies when a MSB fails to maintain a federally insured depository account as required by s. 560.309, F.S., The bill amends this provision to include when a MSB fails to maintain a federally insured depository account as required by s. 560.208, F.S., in addition to s. 560.309, F.S., already referenced in current law.

Financial Institutions Director and Officer Qualifications

Sections 13 and 14 of the bill modifies when the OFR must approve an application for the creation of a banking or trust corporation to require at least two of the proposed directors who are not also proposed officers, and the proposed president or chief executive officer, to have at least one year of direct experience as an executive officer, regulator, or director within the last 10 years, rather than within the last five years. The bill requires, rather than authorizes, the OFR to waive this experience requirement for the proposed president or chief executive officer after considering the specified criteria in current law.[136]

Similarly, directors' minimum qualifications are amended to require (a) in the case of a bank or trust company with a total assets of less than $150 million, at least one director, and (b) 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 at least one year of direct experience as an executive officer, regulator, or director of a financial institution within the 10 years, rather than the last five years.

Credit Unions

Member Qualifications and Meetings

Section 10 of the bill reduces the number of individuals who apply to organize a credit union that must reside in the state from all individuals to a majority of individuals.

Section 11 of the bill removes investment restrictions in real estate and equipment for the credit union. The section also allows credit union members to meet electronically for annual and special meetings and without an in-person quorum and provides virtual attendance may satisfy quorum requirements, subject to the credit union's bylaws.

Investments

Section 12 of the bill repeals a provision that provides a credit union may invest only up to five percent of the credit union's capital in real estate and improvements, furniture, fixtures, and equipment utilized by the credit union for the transaction of business. A related provision is also repealed allowing credit unions to exceed the five percent limit with prior written approval by the OFR if all the specified criteria are met. This amendment is intended to make state credit unions more competitive with federal credit unions that no longer must comply with similar requirements. Further, the OFR reports that the "NCUA's examination and supervision program will address credit unions' safe and sound management of fixed assets."[137]

Examination costs

Sections 9 and 15 of the bill extend the time for a financial institution and family trust company to pay staff examination costs from 30 to 45 days.

---

[136] *Supra* note 76.

[137] The OFR, *2025 Agency Legislative Bill Analysis for SB 1612* (March 10, 2025) (on file with Senate Committee on Banking and Insurance).

Section 16 of the bill amends s. 517.12(21), F.S., to update a cross-reference.

Section 17 provides the bill is effective July 1, 2026.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The bill does not impact state revenues or expenditures.[138]

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

[138] The OFR, *2026 Agency Legislative Bill Analysis for SB 540* (Dec. 29, 2025), p. 5, (on file with the Senate Committee on Banking and Insurance).

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 494.00255, 517.021, 517.061, 520.135, 560.114, 655.045, 657.005, 657.024, 657.042, 658.21, 658.33, 662.141, and 517.12.

This bill creates the following sections of the Florida Statutes: 494.00123, 560.1311, and 655.0171.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Banking and Insurance Committee on January 13, 2026:

- Provides that parties' rights and obligations relating to a surrendered or repossessed motor vehicle are governed exclusively by the Uniform Commercial Code;
- Clarifies that credit union annual and special meetings held virtually do not require a quorum in-person;
- Allows credit unions to consider virtual attendees to satisfy quorum requirements for annual and special meetings held virtually;
- Clarifies when a person meets a definition of "family office" for purposes of an exemption as an investment adviser and an exemption from registration requirements for an offer or sale of securities; and
- Removes **Section 4** of the bill that modifies the Financial Technology Sandbox provisions.

B. Amendments:

None.