By Senator DiCeglie

18-01808-25 20251216__

A bill to be entitled

An act relating to cybersecurity of mortgage brokers and lenders and money services businesses; creating ss. 494.00170 and 560.1215, F.S.; defining terms; requiring licensees to develop and maintain a specified information security program; requiring that such program meet certain criteria; requiring licensees to establish a specified incident response plan; providing requirements for such plan; providing applicability; specifying that a licensee has a specified timeframe to comply with certain provisions; requiring the licensee to maintain a copy of the information security program for a specified period of time; requiring such program to be available upon request or examination; requiring licensees to make a prompt investigation of a cybersecurity event that has occurred or may occur; specifying requirements for such investigation; requiring licensees to complete an investigation or confirm and document that a third-party service provider has completed an investigation under certain circumstances; requiring the licensee to maintain specified records and documentation for a specified period of time; requiring the licensee to produce such records and documentation to be available upon request; requiring licensees to provide a specified notice to the Office of Financial Regulation; requiring the licensee to provide a quarterly update of the investigation under certain circumstances; providing construction; authorizing the

Financial Services Commission to adopt rules; amending ss. 494.00255 and 560.114, F.S.; revising the actions that constitute grounds for disciplinary actions for mortgage brokers and lenders and grounds for the issuance of a cease and desist order or removal order or the denial, suspension, or revocation of a license of a money service business, respectively; providing an effective date.

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

Section 1. Section 494.00170, Florida Statutes, is created to read:

494.00170 Cybersecurity.—

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

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

(b) "Customer information" means any record containing nonpublic personal information about a customer of a financial transaction, whether in paper, electronic, or other form, 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 or process control system, telephone switching and private branch exchange system, or environmental control system which contains customer information or is connected to a system that contains customer information.

(g)1. "Nonpublic personal information" includes all of the following:

a. Personally identifiable financial information.

b. Any list, description, or grouping of customers derived from personally identifiable financial information that is not publicly available. The term includes lists of customers' names and street addresses which are derived, in whole or in part, from personally identifiable information, such as account numbers.

2. The term does not include any of the following:

a. Publicly available information, unless it is part of a list described in sub-subparagraph 1.b.

b. Any list, description, or grouping of customers, along with their publicly available information, if the list was created without using any personally identifiable financial information that is not publicly available. A list of customers' names and addresses is not considered nonpublic personal

information if it contains only publicly available information, is not derived in whole or in part from nonpublic personally identifiable financial information, and is not disclosed in a way that indicates any of the customers on the list are customers of the licensee.

(h)1. "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 submitted on an application for a loan or other financial product or service;

b. A licensee receives about a customer during or as a result of any transaction involving a financial product or service, including information collected through an Internet cookie or from a web server; or

c. A licensee otherwise obtains about a customer in connection with providing a financial product or service, such as records indicating that a customer has previously engaged with the licensee or obtained a financial product or service.

2. Personally identifiable financial information does not include any of the following:

a. A list of names and addresses of customers of an entity that is not a mortgage broker or lender.

b. Information that does not identify a customer, such as aggregate information or anonymized data that does not contain personal identifiers such as account numbers, names, or addresses.

(i)1. "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from any of the

following:

a. Federal, state, or local government records, such as real estate records or security interest filings.

b. Widely distributed media, including telephone directories, television or radio programs, newspapers, or websites that are 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.

c. Disclosures to the general public that are required to be made by federal, state, or local law.

2. For the purpose of this paragraph, the term "reasonable basis to believe is lawfully made available to the general public" means that the licensee has taken steps to determine all of the following:

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.

b. Whether an individual can direct that the information not be made available to the general public and, if so, whether the customer to whom the information relates has so directed.

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

(2)(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) A licensee must ensure the information security program meets all of the following criteria:

1. Is commensurate with the following measures:

a. The size and complexity of the licensee.

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

c. The sensitivity of the nonpublic personal information used by the licensee or in the possession, custody, or control of the licensee.

2. Is designed to:

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; and

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

3. Defines and periodically reevaluates 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 applicable law.

4. Regularly tests and monitors systems and procedures for the detection of actual and attempted attacks on, or intrusions into, the information system.

5. Monitors, evaluates, and adjusts, as necessary, the licensee's information security program to:

a. Ensure the program remains consistent with relevant changes in technology;

b. Confirm that the program accounts for the sensitivity of nonpublic personal information;

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

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

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

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

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

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

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

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

6. Documentation and reporting regarding cybersecurity events and related incident response activities.

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

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

(d) This subsection does not apply to a licensee that:

1. Has fewer than 20 persons on its workforce, including employees and independent contractors; or

2. Has fewer than 500 customers during a calendar year.

(e) A licensee has 180 calendar days from the date the licensee no longer qualifies for exemption under paragraph (d) to comply with this section.

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

(b) During the investigation, the licensee, or the outside vendor or third-party service provider the licensee has

designated to act on its behalf, shall, at a minimum, determine all of the following, to the extent possible:

1. Whether a cybersecurity event has occurred.

2. The date the cybersecurity event first occurred.

3. The nature and scope of the cybersecurity event.

4. Any nonpublic personal information that may have been compromised.

5. Reasonable measures to restore the security of compromised information systems and prevent further unauthorized access, disclosure, or use of nonpublic personal information in the possession, custody, or control of the licensee, outside vendor, or third-party service provider.

(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 must 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 from the date of the event and shall produce the records and documentation upon the office’s request.

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

(b) A licensee shall, upon request by the office, provide a quarterly update of the investigation undertaken pursuant to subsection (3), until conclusion of the investigation.

(5) 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 that term is defined in s. 501.171(1)(b), such covered entity remains subject to s. 501.171.

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

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:

(z) Failure to comply with the notification requirements in s. 494.00170(4).

Section 3. Section 560.1215, Florida Statutes, is created to read:

560.1215 Cybersecurity.—

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

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

(b) "Customer information" means any record containing nonpublic personal information about a customer of a financial

transaction, whether in paper, electronic, or other form, 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 or process control system, telephone switching and private branch exchange system, or environmental control system, which contains customer information or which is connected to a system that contains customer information.

(g)1. "Nonpublic personal information" includes all of the following:

a. Personally identifiable financial information.

b. Any list, description, or grouping of customers derived from personally identifiable financial information that is not publicly available. The term includes lists of customers' names and street addresses which are derived, in whole or in part, from personally identifiable information, such as account

numbers.

2. The term does not include any of the following:

a. Publicly available information, unless it is part of a list described in sub-subparagraph 1.b.

b. Any list, description, or grouping of customers, along with their publicly available information, if the list was created without using any personally identifiable financial information that is not publicly available. A list of customers' names and addresses is not considered nonpublic personal information if it contains only publicly available information, is not derived in whole or in part from nonpublic personally identifiable financial information, and is not disclosed in a way that indicates any of the customers on the list are customers of the licensee.

(h)1. "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 submitted on an application for a loan or other financial product or service;

b. A licensee receives about a customer during or as a result of any transaction involving a financial product or service, including information collected through an internet cookie or from a web server; or

c. A licensee otherwise obtains about a customer in connection with providing a financial product or service, such as records indicating that a customer has previously engaged with the licensee or obtained a financial product or service.

2. Personally identifiable financial information does not include any of the following:

a. A list of names and addresses of customers of an entity that is not a money service business.

b. Information that does not identify a customer, such as aggregate information or anonymized data that does not contain personal identifiers such as account numbers, names, or addresses.

(i)1. "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from any of the following:

a. Federal, state, or local government records, such as real estate records or security interest filings.

b. Widely distributed media, including telephone directories, television or radio programs, newspapers, or websites, that are 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.

c. Disclosures to the general public that are required to be made by federal, state, or local law.

2. For the purpose of this paragraph, the term "reasonable basis to believe is lawfully made available to the general public" means that the licensee has taken steps to determine all of the following:

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.

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.

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

(2)(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) A licensee must ensure the information security program meets all of the following criteria:

1. Is commensurate with the following measures:

a. The size and complexity of the licensee.

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

c. The sensitivity of the nonpublic personal information used by the licensee or in the possession, custody, or control of the licensee.

2. Is designed to:

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; and

c. Protect against unauthorized access to or use of

nonpublic personal information and minimize the likelihood of harm to any customer.

3. Defines and periodically reevaluates 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 applicable law.

4. Regularly tests and monitors systems and procedures for the detection of actual and attempted attacks on, or intrusions into, the information system.

5. Monitors, evaluates, and adjusts, as necessary, the licensee's information security program to:

a. Ensure the program remains consistent with relevant changes in technology;

b. Confirm that the program accounts for the sensitivity of nonpublic personal information;

c. Identify and address changes that may be necessary to the licensee's information systems;

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

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) As part of a licensee's information security program, a licensee shall establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic personal information in the licensee's possession, the licensee's information systems,

or the continuing functionality of any aspect of the licensee's operations. The written incident response plan must address all of the following:

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

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

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

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

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

6. Documentation and reporting regarding cybersecurity events and related incident response activities.

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

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

(d) This subsection does not apply to a licensee that:

1. Has fewer than 20 persons on its workforce, including employees and independent contractors; or

2. Has fewer than 500 customers during a calendar year.

(e) A licensee has 180 calendar days from the date the licensee no longer qualifies for exemption under paragraph (2)(d) to comply with this section.

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

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

1. Whether a cybersecurity event has occurred.

2. The date the cybersecurity event first occurred.

3. The nature and scope of the cybersecurity event.

4. Any nonpublic personal information that may have been compromised.

5. Reasonable measures to restore the security of compromised information systems and prevent further unauthorized access, disclosure, or use of nonpublic personal information in the possession, custody, or control of the licensee, outside vendor, or third-party service provider.

(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 must 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 from the date of the event and shall produce the records and documentation upon the office's request.

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

(b) A licensee, shall, upon request by the office, provide a quarterly update of the investigation undertaken pursuant to paragraph (3), until conclusion of the investigation.

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

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

Section 4. Paragraph (dd) is added to subsection (1) of section 560.114, Florida Statutes, to read:

560.114 Disciplinary actions; penalties.—

(1) The following actions by a money services business, authorized vendor, or affiliated party 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:

(dd) Failure to comply with the notification requirements

in s. 560.1215(4).

Section 5. This act shall take effect July 1, 2025.