

By Senator DiCeglie

18-01808-25

20251216\_\_

1                                   A bill to be entitled  
2       An act relating to cybersecurity of mortgage brokers  
3       and lenders and money services businesses; creating  
4       ss. 494.00170 and 560.1215, F.S.; defining terms;  
5       requiring licensees to develop and maintain a  
6       specified information security program; requiring that  
7       such program meet certain criteria; requiring  
8       licensees to establish a specified incident response  
9       plan; providing requirements for such plan; providing  
10      applicability; specifying that a licensee has a  
11      specified timeframe to comply with certain provisions;  
12      requiring the licensee to maintain a copy of the  
13      information security program for a specified period of  
14      time; requiring such program to be available upon  
15      request or examination; requiring licensees to make a  
16      prompt investigation of a cybersecurity event that has  
17      occurred or may occur; specifying requirements for  
18      such investigation; requiring licensees to complete an  
19      investigation or confirm and document that a third-  
20      party service provider has completed an investigation  
21      under certain circumstances; requiring the licensee to  
22      maintain specified records and documentation for a  
23      specified period of time; requiring the licensee to  
24      produce such records and documentation to be available  
25      upon request; requiring licensees to provide a  
26      specified notice to the Office of Financial  
27      Regulation; requiring the licensee to provide a  
28      quarterly update of the investigation under certain  
29      circumstances; providing construction; authorizing the

18-01808-25

20251216\_\_

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

38  
39 Be It Enacted by the Legislature of the State of Florida:

40  
41 Section 1. Section 494.00170, Florida Statutes, is created  
42 to read:

43 494.00170 Cybersecurity.-

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

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

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

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

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

18-01808-25

20251216\_\_

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

63       (f) "Information system" means a discrete set of electronic  
64 information resources organized for the collection, processing,  
65 maintenance, use, sharing, dissemination, or disposition of  
66 electronic information, as well as any specialized system such  
67 as an industrial or process control system, telephone switching  
68 and private branch exchange system, or environmental control  
69 system which contains customer information or is connected to a  
70 system that contains customer information.

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

73       a. Personally identifiable financial information.

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

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

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

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

18-01808-25

20251216\_\_

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

93 (h)1. "Personally identifiable financial information" means  
94 any information that:

95 a. A customer provides to a licensee to obtain a financial  
96 product or service, such as information submitted on an  
97 application for a loan or other financial product or service;

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

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

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

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

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

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

18-01808-25

20251216\_\_

117 following:

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

120 b. Widely distributed media, including telephone  
121 directories, television or radio programs, newspapers, or  
122 websites that are available to the general public on an  
123 unrestricted basis. A website is not restricted merely because  
124 an Internet service provider or a site operator requires a fee  
125 or a password, so long as access is available to the general  
126 public.

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

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

133 a. That the information is of the type that is available to  
134 the general public, such as information included on the public  
135 record in the jurisdiction where the mortgage would be recorded.

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

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

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

18-01808-25

20251216\_\_

146 contains administrative, technical, and physical safeguards for  
147 the protection of the licensee's information system and  
148 nonpublic personal information.

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

151 1. Is commensurate with the following measures:

152 a. The size and complexity of the licensee.

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

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

158 2. Is designed to:

159 a. Protect the security and confidentiality of nonpublic  
160 personal information and the security of the licensee's  
161 information system;

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

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

168 3. Defines and periodically reevaluates the retention  
169 schedule and the mechanism for the destruction of nonpublic  
170 personal information if retention is no longer necessary for the  
171 licensee's business operations or required by applicable law.

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

18-01808-25

20251216\_\_

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

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

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

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

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

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

189 (c) As part of a licensee's information security program, a  
190 licensee shall establish a written incident response plan  
191 designed to promptly respond to, and recover from, a  
192 cybersecurity event that compromises the confidentiality,  
193 integrity, or availability of nonpublic personal information in  
194 the licensee's possession, the licensee's information system, or  
195 the continuing functionality of any aspect of the licensee's  
196 operations. The written incident response plan must address all  
197 of the following:

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

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

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

18-01808-25

20251216\_\_

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

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

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

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

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

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

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

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

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

222 (f) A licensee shall maintain a copy of the information  
223 security program for a minimum of 5 years and shall make it  
224 available to the office upon request or as part of an  
225 examination.

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

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



18-01808-25

20251216\_\_

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

- 235 1. Whether a cybersecurity event has occurred.  
236 2. The date the cybersecurity event first occurred.  
237 3. The nature and scope of the cybersecurity event.  
238 4. Any nonpublic personal information that may have been  
239 compromised.  
240 5. Reasonable measures to restore the security of  
241 compromised information systems and prevent further unauthorized  
242 access, disclosure, or use of nonpublic personal information in  
243 the possession, custody, or control of the licensee, outside  
244 vendor, or third-party service provider.

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

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

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

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

18-01808-25

20251216\_\_

262       (5) This section may not be construed to relieve a covered  
263 entity from complying with s. 501.171. To the extent a licensee  
264 is a covered entity, as that term is defined in s.  
265 501.171(1)(b), such covered entity remains subject to s.  
266 501.171.

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

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

274       494.00255 Administrative penalties and fines; license  
275 violations.—

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

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

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

284       560.1215 Cybersecurity.—

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

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

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

18-01808-25

20251216\_\_

291 transaction, whether in paper, electronic, or other form, which  
292 is handled or maintained by or on behalf of the licensee or its  
293 affiliates.

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

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

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

304 (f) "Information system" means a discrete set of electronic  
305 information resources organized for the collection, processing,  
306 maintenance, use, sharing, dissemination, or disposition of  
307 electronic information, as well as any specialized system, such  
308 as an industrial or process control system, telephone switching  
309 and private branch exchange system, or environmental control  
310 system, which contains customer information or which is  
311 connected to a system that contains customer information.

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

314 a. Personally identifiable financial information.

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

18-01808-25

20251216\_\_

320 numbers.

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

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

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

334 (h)1. "Personally identifiable financial information" means  
335 any information that:

336 a. A customer provides to a licensee to obtain a financial  
337 product or service, such as information submitted on an  
338 application for a loan or other financial product or service;

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

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

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

18-01808-25

20251216\_\_

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

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

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

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

361 b. Widely distributed media, including telephone  
362 directories, television or radio programs, newspapers, or  
363 websites, that are available to the general public on an  
364 unrestricted basis. A website is not restricted merely because  
365 an Internet service provider or a site operator requires a fee  
366 or a password, so long as access is available to the general  
367 public.

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

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

374 a. That the information is of the type that is available to  
375 the general public, such as information included on the public  
376 record in the jurisdiction where the mortgage would be recorded.

377 b. Whether an individual can direct that the information

18-01808-25

20251216\_\_

378 not be made available to the general public and, if so, the  
379 customer to whom the information relates has not done so.

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

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

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

392 1. Is commensurate with the following measures:

393 a. The size and complexity of the licensee.

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

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

399 2. Is designed to:

400 a. Protect the security and confidentiality of nonpublic  
401 personal information and the security of the licensee's  
402 information system;

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

406 c. Protect against unauthorized access to or use of

18-01808-25

20251216\_\_

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

409 3. Defines and periodically reevaluates the retention  
410 schedule and the mechanism for the destruction of nonpublic  
411 personal information if retention is no longer necessary for the  
412 licensee's business operations or required by applicable law.

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

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

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

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

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

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

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

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

18-01808-25

20251216\_\_

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

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

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

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

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

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

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

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

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

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

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

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

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

463 (f) A licensee shall maintain a copy of the information  
464 security program for a minimum of 5 years and shall make it



18-01808-25

20251216\_\_

465 available to the office upon request or as part of an  
466 examination.

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

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

476 1. Whether a cybersecurity event has occurred.  
477 2. The date the cybersecurity event first occurred.  
478 3. The nature and scope of the cybersecurity event.  
479 4. Any nonpublic personal information that may have been  
480 compromised.

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

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

493 (d) A licensee shall maintain all records and documentation

18-01808-25

20251216\_\_

494 related to the licensee's investigation of a cybersecurity event  
495 for a minimum of 5 years from the date of the event and shall  
496 produce the records and documentation upon the office's request.

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

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

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

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

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

515 560.114 Disciplinary actions; penalties.—

516 (1) The following actions by a money services business,  
517 authorized vendor, or affiliated party constitute grounds for  
518 the issuance of a cease and desist order; the issuance of a  
519 removal order; the denial, suspension, or revocation of a  
520 license; or taking any other action within the authority of the  
521 office pursuant to this chapter:

522 (dd) Failure to comply with the notification requirements

18-01808-25

20251216\_\_

523 in s. 560.1215(4).

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