

HOUSE BILL No. 6491

November 8, 2018, Introduced by Rep. Theis and referred to the Committee on Insurance.

A bill to amend 1956 PA 218, entitled
"The insurance code of 1956,"
(MCL 500.100 to 500.8302) by adding chapter 5A.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

CHAPTER 5A

DATA SECURITY

SEC. 550. THIS CHAPTER DOES NOT CREATE OR IMPLY A PRIVATE
CAUSE OF ACTION FOR VIOLATION OF ITS PROVISIONS AND DOES NOT
CURTAIL A PRIVATE CAUSE OF ACTION THAT WOULD OTHERWISE EXIST IN THE
ABSENCE OF THIS CHAPTER. NOTWITHSTANDING ANY OTHER PROVISION OF
LAW, THIS CHAPTER ESTABLISHES THE EXCLUSIVE STANDARDS APPLICABLE TO
LICENSEES FOR DATA SECURITY, THE INVESTIGATION OF A CYBERSECURITY
EVENT, AND NOTIFICATION TO THE DIRECTOR.

SEC. 553. AS USED IN THIS CHAPTER:

1 (A) "AUTHORIZED INDIVIDUAL" MEANS AN INDIVIDUAL KNOWN TO AND
2 SCREENED BY THE LICENSEE AND DETERMINED TO BE NECESSARY AND
3 APPROPRIATE TO HAVE ACCESS TO THE NONPUBLIC INFORMATION HELD BY THE
4 LICENSEE AND ITS INFORMATION SYSTEMS.

5 (B) "CONSUMER" MEANS AN INDIVIDUAL, INCLUDING, BUT NOT LIMITED
6 TO, AN APPLICANT, A POLICYHOLDER, AN INSURED, A BENEFICIARY, A
7 CLAIMANT, AND A CERTIFICATE HOLDER, WHO IS A RESIDENT OF THIS STATE
8 AND WHOSE NONPUBLIC INFORMATION IS IN A LICENSEE'S POSSESSION,
9 CUSTODY, OR CONTROL.

10 (C) "CYBERSECURITY EVENT" MEANS AN EVENT THAT RESULTS IN
11 UNAUTHORIZED ACCESS TO AND ACQUISITION OF, OR DISRUPTION OR MISUSE
12 OF, AN INFORMATION SYSTEM OR NONPUBLIC INFORMATION STORED ON AN
13 INFORMATION SYSTEM. CYBERSECURITY EVENT DOES NOT INCLUDE EITHER OF
14 THE FOLLOWING:

15 (i) THE UNAUTHORIZED ACQUISITION OF ENCRYPTED NONPUBLIC
16 INFORMATION IF THE ENCRYPTION, PROCESS, OR KEY IS NOT ALSO
17 ACQUIRED, RELEASED, OR USED WITHOUT AUTHORIZATION.

18 (ii) THE UNAUTHORIZED ACCESS TO DATA BY A PERSON IF THE ACCESS
19 MEETS ALL OF THE FOLLOWING CRITERIA:

20 (A) THE PERSON ACTED IN GOOD FAITH IN ACCESSING THE DATA.

21 (B) THE ACCESS WAS RELATED TO ACTIVITIES OF THE PERSON.

22 (C) THE PERSON DID NOT MISUSE ANY PERSONAL INFORMATION OR
23 DISCLOSE ANY PERSONAL INFORMATION TO AN UNAUTHORIZED PERSON.

24 (D) "ENCRYPTED" MEANS THE TRANSFORMATION OF DATA INTO A FORM
25 THAT RESULTS IN A LOW PROBABILITY OF ASSIGNING MEANING WITHOUT THE
26 USE OF A PROTECTIVE PROCESS OR KEY.

27 (E) "INFORMATION SECURITY PROGRAM" MEANS THE ADMINISTRATIVE,

1 TECHNICAL, AND PHYSICAL SAFEGUARDS THAT A LICENSEE USES TO ACCESS,
2 COLLECT, DISTRIBUTE, PROCESS, PROTECT, STORE, USE, TRANSMIT,
3 DISPOSE OF, OR OTHERWISE HANDLE NONPUBLIC INFORMATION.

4 (F) "INFORMATION SYSTEM" MEANS A DISCRETE SET OF ELECTRONIC
5 INFORMATION RESOURCES ORGANIZED FOR THE COLLECTION, PROCESSING,
6 MAINTENANCE, USE, SHARING, DISSEMINATION, OR DISPOSITION OF
7 ELECTRONIC NONPUBLIC INFORMATION, AS WELL AS ANY SPECIALIZED SYSTEM
8 SUCH AS AN INDUSTRIAL OR PROCESS CONTROLS SYSTEM, A TELEPHONE
9 SWITCHING AND PRIVATE BRANCH EXCHANGE SYSTEM, OR AN ENVIRONMENTAL
10 CONTROL SYSTEM.

11 (G) "LICENSEE" MEANS A LICENSED INSURER OR PRODUCER, AND OTHER
12 PERSONS LICENSED OR REQUIRED TO BE LICENSED, AUTHORIZED, OR
13 REGISTERED, OR HOLDING OR REQUIRED TO HOLD A CERTIFICATE OF
14 AUTHORITY UNDER THIS ACT. LICENSEE DOES NOT INCLUDE A PURCHASING
15 GROUP OR A RISK RETENTION GROUP CHARTERED AND LICENSED IN A STATE
16 OTHER THAN THIS STATE OR A PERSON THAT IS ACTING AS AN ASSUMING
17 INSURER THAT IS DOMICILED IN ANOTHER STATE OR JURISDICTION.

18 (H) "MULTI-FACTOR AUTHENTICATION" MEANS AUTHENTICATION THROUGH
19 VERIFICATION OF AT LEAST 2 OF THE FOLLOWING TYPES OF AUTHENTICATION
20 FACTORS:

21 (i) KNOWLEDGE FACTORS, SUCH AS A PASSWORD.

22 (ii) POSSESSION FACTORS, SUCH AS A TOKEN OR TEXT MESSAGE ON A
23 MOBILE PHONE.

24 (iii) INHERENCE FACTORS, SUCH AS A BIOMETRIC CHARACTERISTIC.

25 (I) "NONPUBLIC INFORMATION" MEANS ELECTRONIC INFORMATION THAT
26 IS NOT PUBLICLY AVAILABLE INFORMATION AND IS EITHER OF THE
27 FOLLOWING:

(i) ANY INFORMATION CONCERNING A CONSUMER THAT BECAUSE OF NAME, NUMBER, PERSONAL MARK, OR OTHER IDENTIFIER CAN BE USED TO IDENTIFY THE CONSUMER, IN COMBINATION WITH ANY 1 OR MORE OF THE FOLLOWING DATA ELEMENTS:

(A) SOCIAL SECURITY NUMBER.

(B) DRIVER LICENSE NUMBER OR NONDRIVER IDENTIFICATION CARD NUMBER.

(C) FINANCIAL ACCOUNT NUMBER, OR CREDIT OR DEBIT CARD NUMBER.

(D) ANY SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO A CONSUMER'S FINANCIAL ACCOUNT.

(E) BIOMETRIC RECORDS.

(ii) ANY INFORMATION OR DATA, EXCEPT AGE OR GENDER, IN ANY FORM OR MEDIUM CREATED BY OR DERIVED FROM A HEALTH CARE PROVIDER OR A CONSUMER, THAT CAN BE USED TO IDENTIFY A PARTICULAR CONSUMER, AND THAT RELATES TO ANY OF THE FOLLOWING:

(A) THE PAST, PRESENT, OR FUTURE PHYSICAL, MENTAL, OR BEHAVIORAL HEALTH OR CONDITION OF ANY CONSUMER OR A MEMBER OF THE CONSUMER'S FAMILY.

(B) THE PROVISION OF HEALTH CARE TO ANY CONSUMER.

(C) PAYMENT FOR THE PROVISION OF HEALTH CARE TO ANY CONSUMER.

(J) "PUBLICLY AVAILABLE INFORMATION" MEANS ANY INFORMATION THAT A LICENSEE HAS A REASONABLE BASIS TO BELIEVE IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS BY WIDE DISTRIBUTION BY THE MEDIA OR BY DISCLOSURES TO THE GENERAL PUBLIC THAT ARE REQUIRED TO BE MADE BY FEDERAL, STATE, OR LOCAL LAW. A LICENSEE HAS A REASONABLE BASIS TO BELIEVE THAT INFORMATION IS LAWFULLY MADE AVAILABLE TO THE GENERAL

1 PUBLIC IF BOTH OF THE FOLLOWING APPLY:

2 (i) THE LICENSEE HAS TAKEN STEPS TO DETERMINE THAT THE
3 INFORMATION IS OF THE TYPE THAT IS AVAILABLE TO THE GENERAL PUBLIC.

4 (ii) IF AN INDIVIDUAL CAN DIRECT THAT THE INFORMATION NOT BE
5 MADE AVAILABLE TO THE GENERAL PUBLIC, THAT THE LICENSEE'S CONSUMER
6 HAS NOT DIRECTED THAT THE INFORMATION NOT BE MADE AVAILABLE TO THE
7 GENERAL PUBLIC.

8 (K) "RISK ASSESSMENT" MEANS THE RISK ASSESSMENT THAT EACH
9 LICENSEE IS REQUIRED TO CONDUCT UNDER SECTION 555(3).

10 (l) "THIRD-PARTY SERVICE PROVIDER" MEANS A PERSON THAT IS NOT
11 A LICENSEE AND THAT CONTRACTS WITH A LICENSEE TO MAINTAIN, PROCESS,
12 OR STORE, OR OTHERWISE IS PERMITTED ACCESS TO NONPUBLIC
13 INFORMATION, THROUGH ITS PROVISION OF SERVICES TO THE LICENSEE.

14 SEC. 555. (1) COMMENSURATE WITH THE SIZE AND COMPLEXITY OF THE
15 LICENSEE, THE NATURE AND SCOPE OF THE LICENSEE'S ACTIVITIES,
16 INCLUDING ITS USE OF THIRD-PARTY SERVICE PROVIDERS, AND THE
17 SENSITIVITY OF THE NONPUBLIC INFORMATION USED BY THE LICENSEE OR IN
18 THE LICENSEE'S POSSESSION, CUSTODY, OR CONTROL, EACH LICENSEE SHALL
19 DEVELOP, IMPLEMENT, AND MAINTAIN A COMPREHENSIVE WRITTEN
20 INFORMATION SECURITY PROGRAM, BASED ON THE LICENSEE'S RISK
21 ASSESSMENT, THAT CONTAINS ADMINISTRATIVE, TECHNICAL, AND PHYSICAL
22 SAFEGUARDS FOR THE PROTECTION OF NONPUBLIC INFORMATION AND THE
23 LICENSEE'S INFORMATION SYSTEM.

24 (2) A LICENSEE'S INFORMATION SECURITY PROGRAM MUST BE DESIGNED
25 TO DO ALL OF THE FOLLOWING:

26 (A) PROTECT THE SECURITY AND CONFIDENTIALITY OF NONPUBLIC
27 INFORMATION AND THE SECURITY OF THE INFORMATION SYSTEM.

1 (B) PROTECT AGAINST ANY THREATS OR HAZARDS TO THE SECURITY OR
2 INTEGRITY OF NONPUBLIC INFORMATION AND THE INFORMATION SYSTEM.

3 (C) PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF NONPUBLIC
4 INFORMATION, AND MINIMIZE THE LIKELIHOOD OF HARM TO ANY CONSUMER.

5 (D) MAINTAIN POLICIES AND PROCEDURES FOR THE SECURE DISPOSAL
6 ON A PERIODIC BASIS OF ANY NONPUBLIC INFORMATION THAT IS NO LONGER
7 NECESSARY FOR BUSINESS OPERATIONS OR FOR OTHER LEGITIMATE BUSINESS
8 PURPOSES.

9 (3) A LICENSEE SHALL DO ALL OF THE FOLLOWING:

10 (A) DESIGNATE 1 OR MORE EMPLOYEES, AN AFFILIATE, OR AN OUTSIDE
11 VENDOR TO ACT ON BEHALF OF THE LICENSEE THAT IS RESPONSIBLE FOR THE
12 INFORMATION SECURITY PROGRAM.

13 (B) IDENTIFY REASONABLY FORESEEABLE INTERNAL OR EXTERNAL
14 THREATS THAT COULD RESULT IN UNAUTHORIZED ACCESS, TRANSMISSION,
15 DISCLOSURE, MISUSE, ALTERATION, OR DESTRUCTION OF NONPUBLIC
16 INFORMATION, INCLUDING THE SECURITY OF INFORMATION SYSTEMS AND
17 NONPUBLIC INFORMATION THAT ARE ACCESSIBLE TO, OR HELD BY, THIRD-
18 PARTY SERVICE PROVIDERS.

19 (C) ASSESS THE LIKELIHOOD AND POTENTIAL DAMAGE OF THESE
20 THREATS, TAKING INTO CONSIDERATION THE SENSITIVITY OF THE NONPUBLIC
21 INFORMATION.

22 (D) ASSESS THE SUFFICIENCY OF POLICIES, PROCEDURES,
23 INFORMATION SYSTEMS, AND OTHER SAFEGUARDS IN PLACE TO MANAGE THESE
24 THREATS, INCLUDING CONSIDERATION OF THREATS IN EACH RELEVANT AREA
25 OF THE LICENSEE'S OPERATIONS, INCLUDING ALL OF THE FOLLOWING:

26 (i) EMPLOYEE TRAINING AND MANAGEMENT.

27 (ii) INFORMATION SYSTEMS, INCLUDING NETWORK AND SOFTWARE

1 DESIGN, AS WELL AS INFORMATION CLASSIFICATION, GOVERNANCE,
2 PROCESSING, STORAGE, TRANSMISSION, AND DISPOSAL.

3 (iii) DETECTING, PREVENTING, AND RESPONDING TO ATTACKS,
4 INTRUSIONS, OR OTHER SYSTEMS FAILURES.

5 (E) IMPLEMENT INFORMATION SAFEGUARDS TO MANAGE THE THREATS
6 IDENTIFIED IN ITS ONGOING ASSESSMENT, AND, NO LESS THAN ANNUALLY,
7 ASSESS THE EFFECTIVENESS OF THE SAFEGUARDS' KEY CONTROLS, SYSTEMS,
8 AND PROCEDURES.

9 (4) BASED ON ITS RISK ASSESSMENT, A LICENSEE SHALL DO ALL OF
10 THE FOLLOWING:

11 (A) DESIGN ITS INFORMATION SECURITY PROGRAM TO MITIGATE THE
12 IDENTIFIED RISKS, COMMENSURATE WITH THE SIZE AND COMPLEXITY OF THE
13 LICENSEE, THE NATURE AND SCOPE OF THE LICENSEE'S ACTIVITIES,
14 INCLUDING ITS USE OF THIRD-PARTY SERVICE PROVIDERS, AND THE
15 SENSITIVITY OF THE NONPUBLIC INFORMATION USED BY THE LICENSEE OR IN
16 THE LICENSEE'S POSSESSION, CUSTODY, OR CONTROL.

17 (B) DETERMINE WHICH OF THE FOLLOWING SECURITY MEASURES ARE
18 APPROPRIATE AND IMPLEMENT THOSE APPROPRIATE SECURITY MEASURES:

19 (i) PLACING ACCESS CONTROLS ON INFORMATION SYSTEMS, INCLUDING
20 CONTROLS TO AUTHENTICATE AND PERMIT ACCESS ONLY TO AUTHORIZED
21 INDIVIDUALS TO PROTECT AGAINST THE UNAUTHORIZED ACQUISITION OF
22 NONPUBLIC INFORMATION.

23 (ii) IDENTIFYING AND MANAGING THE DATA, PERSONNEL, DEVICES,
24 SYSTEMS, AND FACILITIES THAT ENABLE THE ORGANIZATION TO ACHIEVE
25 BUSINESS PURPOSES IN ACCORDANCE WITH THEIR RELATIVE IMPORTANCE TO
26 BUSINESS OBJECTIVES AND THE ORGANIZATION'S RISK STRATEGY.

27 (iii) RESTRICTING PHYSICAL ACCESS TO NONPUBLIC INFORMATION TO

1 AUTHORIZED INDIVIDUALS ONLY.

2 (iv) PROTECTING BY ENCRYPTION OR OTHER APPROPRIATE MEANS ALL
3 NONPUBLIC INFORMATION WHILE BEING TRANSMITTED OVER AN EXTERNAL
4 NETWORK AND ALL NONPUBLIC INFORMATION STORED ON A LAPTOP COMPUTER
5 OR OTHER PORTABLE COMPUTING OR STORAGE DEVICE OR MEDIA.

6 (v) ADOPTING SECURE DEVELOPMENT PRACTICES FOR IN-HOUSE
7 DEVELOPED APPLICATIONS UTILIZED BY THE LICENSEE.

8 (vi) MODIFYING THE INFORMATION SYSTEM IN ACCORDANCE WITH THE
9 LICENSEE'S INFORMATION SECURITY PROGRAM.

10 (vii) USING EFFECTIVE CONTROLS, WHICH MAY INCLUDE MULTI-FACTOR
11 AUTHENTICATION PROCEDURES FOR EMPLOYEES ACCESSING NONPUBLIC
12 INFORMATION.

13 (viii) REGULARLY TESTING AND MONITORING SYSTEMS AND PROCEDURES
14 TO DETECT ACTUAL AND ATTEMPTED ATTACKS ON, OR INTRUSIONS INTO,
15 INFORMATION SYSTEMS.

16 (ix) INCLUDING AUDIT TRAILS WITHIN THE INFORMATION SECURITY
17 PROGRAM DESIGNED TO DETECT AND RESPOND TO CYBERSECURITY EVENTS AND
18 DESIGNED TO RECONSTRUCT MATERIAL FINANCIAL TRANSACTIONS SUFFICIENT
19 TO SUPPORT NORMAL OPERATIONS AND OBLIGATIONS OF THE LICENSEE.

20 (x) IMPLEMENTING MEASURES TO PROTECT AGAINST DESTRUCTION,
21 LOSS, OR DAMAGE OF NONPUBLIC INFORMATION DUE TO ENVIRONMENTAL
22 HAZARDS, SUCH AS FIRE AND WATER DAMAGE OR OTHER CATASTROPHES OR
23 TECHNOLOGICAL FAILURES.

24 (xi) DEVELOPING, IMPLEMENTING, AND MAINTAINING PROCEDURES FOR
25 THE SECURE DISPOSAL OF NONPUBLIC INFORMATION IN ANY FORMAT.

26 (C) INCLUDE CYBERSECURITY RISKS IN THE LICENSEE'S ENTERPRISE
27 RISK MANAGEMENT PROCESS.

1 (D) STAY INFORMED REGARDING EMERGING THREATS OR
2 VULNERABILITIES AND UTILIZE REASONABLE SECURITY MEASURES WHEN
3 SHARING INFORMATION RELATIVE TO THE CHARACTER OF THE SHARING AND
4 THE TYPE OF INFORMATION SHARED.

5 (E) PROVIDE ITS PERSONNEL WITH CYBERSECURITY AWARENESS
6 TRAINING THAT IS UPDATED AS NECESSARY TO REFLECT RISKS IDENTIFIED
7 BY THE LICENSEE IN THE RISK ASSESSMENT.

8 (5) IF A LICENSEE HAS A BOARD OF DIRECTORS, THE BOARD OR AN
9 APPROPRIATE COMMITTEE OF THE BOARD SHALL, AT A MINIMUM, DO ALL OF
10 THE FOLLOWING:

11 (A) REQUIRE THE LICENSEE'S EXECUTIVE MANAGEMENT OR ITS
12 DELEGATES TO DEVELOP, IMPLEMENT, AND MAINTAIN THE LICENSEE'S
13 INFORMATION SECURITY PROGRAM.

14 (B) REQUIRE THE LICENSEE'S EXECUTIVE MANAGEMENT OR ITS
15 DELEGATES TO REPORT IN WRITING, AT LEAST ANNUALLY, ALL OF THE
16 FOLLOWING INFORMATION:

17 (i) THE OVERALL STATUS OF THE INFORMATION SECURITY PROGRAM AND
18 THE LICENSEE'S COMPLIANCE WITH THIS CHAPTER.

19 (ii) MATERIAL MATTERS RELATED TO THE INFORMATION SECURITY
20 PROGRAM, ADDRESSING ISSUES SUCH AS RISK ASSESSMENT, RISK MANAGEMENT
21 AND CONTROL DECISIONS, RESULTS OF TESTING, CYBERSECURITY EVENTS OR
22 VIOLATIONS, AND MANAGEMENT'S RESPONSES TO THE MATERIAL MATTERS
23 DESCRIBED IN THIS SUBPARAGRAPH, AND RECOMMENDATIONS FOR CHANGES IN
24 THE INFORMATION SECURITY PROGRAM.

25 (iii) IF EXECUTIVE MANAGEMENT DELEGATES ANY OF ITS
26 RESPONSIBILITIES UNDER THIS SECTION, IT SHALL OVERSEE THE
27 DEVELOPMENT, IMPLEMENTATION, AND MAINTENANCE OF THE LICENSEE'S

1 INFORMATION SECURITY PROGRAM PREPARED BY A DELEGATE AND SHALL
2 RECEIVE A REPORT FROM THE DELEGATE COMPLYING WITH THE REQUIREMENTS
3 OF THE REPORT TO THE BOARD OF DIRECTORS.

4 (6) A LICENSEE SHALL EXERCISE DUE DILIGENCE IN SELECTING ITS
5 THIRD-PARTY SERVICE PROVIDER. A LICENSEE SHALL REQUIRE A THIRD-
6 PARTY SERVICE PROVIDER TO IMPLEMENT APPROPRIATE ADMINISTRATIVE,
7 TECHNICAL, AND PHYSICAL MEASURES TO PROTECT AND SECURE THE
8 INFORMATION SYSTEMS AND NONPUBLIC INFORMATION THAT ARE ACCESSIBLE
9 TO, OR HELD BY, THE THIRD-PARTY SERVICE PROVIDER.

10 (7) A LICENSEE SHALL MONITOR, EVALUATE, AND ADJUST, AS
11 APPROPRIATE, THE INFORMATION SECURITY PROGRAM CONSISTENT WITH ANY
12 RELEVANT CHANGES IN TECHNOLOGY, THE SENSITIVITY OF ITS NONPUBLIC
13 INFORMATION, INTERNAL OR EXTERNAL THREATS TO INFORMATION, AND THE
14 LICENSEE'S OWN CHANGING BUSINESS ARRANGEMENTS, SUCH AS MERGERS AND
15 ACQUISITIONS, ALLIANCES AND JOINT VENTURES, OUTSOURCING
16 ARRANGEMENTS, AND CHANGES TO INFORMATION SYSTEMS.

17 (8) AS PART OF ITS INFORMATION SECURITY PROGRAM, EACH LICENSEE
18 SHALL ESTABLISH A WRITTEN INCIDENT RESPONSE PLAN DESIGNED TO
19 PROMPTLY RESPOND TO, AND RECOVER FROM, ANY CYBERSECURITY EVENT THAT
20 COMPROMISES THE CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY OF
21 NONPUBLIC INFORMATION IN ITS POSSESSION, THE LICENSEE'S INFORMATION
22 SYSTEMS, OR THE CONTINUING FUNCTIONALITY OF ANY ASPECT OF THE
23 LICENSEE'S BUSINESS OR OPERATIONS. AN INCIDENT RESPONSE PLAN UNDER
24 THIS SUBSECTION MUST ADDRESS ALL OF THE FOLLOWING AREAS:

25 (A) THE INTERNAL PROCESS FOR RESPONDING TO A CYBERSECURITY
26 EVENT.

27 (B) THE GOALS OF THE INCIDENT RESPONSE PLAN.

1 (C) THE DEFINITION OF CLEAR ROLES, RESPONSIBILITIES, AND
2 LEVELS OF DECISION-MAKING AUTHORITY.

3 (D) EXTERNAL AND INTERNAL COMMUNICATIONS AND INFORMATION
4 SHARING.

5 (E) IDENTIFICATION OF REQUIREMENTS FOR THE REMEDIATION OF ANY
6 IDENTIFIED WEAKNESSES IN INFORMATION SYSTEMS AND ASSOCIATED
7 CONTROLS.

8 (F) DOCUMENTATION AND REPORTING REGARDING CYBERSECURITY EVENTS
9 AND RELATED INCIDENT RESPONSE ACTIVITIES.

10 (G) THE EVALUATION AND REVISION AS NECESSARY OF THE INCIDENT
11 RESPONSE PLAN FOLLOWING A CYBERSECURITY EVENT.

12 (9) BY FEBRUARY 15 OF EACH YEAR, EACH INSURER DOMICILED IN
13 THIS STATE SHALL SUBMIT TO THE DIRECTOR A WRITTEN STATEMENT,
14 CERTIFYING THAT THE INSURER IS IN COMPLIANCE WITH THE REQUIREMENTS
15 OF THIS SECTION. EACH INSURER SHALL MAINTAIN FOR EXAMINATION BY THE
16 DEPARTMENT ALL RECORDS, SCHEDULES, AND DATA SUPPORTING THIS
17 CERTIFICATE FOR 5 YEARS. TO THE EXTENT AN INSURER HAS IDENTIFIED
18 AREAS, SYSTEMS, OR PROCESSES THAT REQUIRE MATERIAL IMPROVEMENT,
19 UPDATING, OR REDESIGN, THE INSURER SHALL DOCUMENT THE
20 IDENTIFICATION AND THE REMEDIAL EFFORTS PLANNED AND UNDERWAY TO
21 ADDRESS THE AREAS, SYSTEMS, OR PROCESSES. THE DOCUMENTATION
22 DESCRIBED IN THIS SUBSECTION MUST BE AVAILABLE FOR INSPECTION BY
23 THE DIRECTOR.

24 SEC. 557. (1) IF THE LICENSEE LEARNS THAT A CYBERSECURITY
25 EVENT HAS OR MAY HAVE OCCURRED, THE LICENSEE OR AN OUTSIDE VENDOR
26 OR SERVICE PROVIDER, OR BOTH, DESIGNATED TO ACT ON BEHALF OF THE
27 LICENSEE, SHALL CONDUCT A PROMPT INVESTIGATION.

1 (2) DURING THE INVESTIGATION UNDER SUBSECTION (1), THE
2 LICENSEE, OR AN OUTSIDE VENDOR OR SERVICE PROVIDER, OR BOTH,
3 DESIGNATED TO ACT ON BEHALF OF THE LICENSEE, SHALL, AT A MINIMUM,
4 DO AS MUCH OF THE FOLLOWING AS POSSIBLE:

5 (A) DETERMINE WHETHER A CYBERSECURITY EVENT HAS OCCURRED.

6 (B) ASSESS THE NATURE AND SCOPE OF THE CYBERSECURITY EVENT.

7 (C) IDENTIFY ANY NONPUBLIC INFORMATION THAT MAY HAVE BEEN
8 INVOLVED IN THE CYBERSECURITY EVENT.

9 (D) PERFORM OR OVERSEE REASONABLE MEASURES TO RESTORE THE
10 SECURITY OF THE INFORMATION SYSTEMS COMPROMISED IN THE
11 CYBERSECURITY EVENT TO PREVENT FURTHER UNAUTHORIZED ACQUISITION,
12 RELEASE, OR USE OF NONPUBLIC INFORMATION IN THE LICENSEE'S
13 POSSESSION, CUSTODY, OR CONTROL.

14 (3) THE LICENSEE SHALL MAINTAIN RECORDS CONCERNING ALL
15 CYBERSECURITY EVENTS FOR AT LEAST 5 YEARS FROM THE DATE OF THE
16 CYBERSECURITY EVENT AND SHALL PRODUCE THOSE RECORDS ON DEMAND OF
17 THE DIRECTOR.

18 SEC. 559. (1) EACH LICENSEE SHALL NOTIFY THE DIRECTOR AS
19 PROMPTLY AS POSSIBLE BUT NOT LATER THAN 10 BUSINESS DAYS AFTER A
20 DETERMINATION THAT A CYBERSECURITY EVENT INVOLVING NONPUBLIC
21 INFORMATION THAT IS IN THE POSSESSION OF A LICENSEE HAS OCCURRED
22 WHEN EITHER OF THE FOLLOWING CRITERIA HAS BEEN MET:

23 (A) THIS STATE IS THE LICENSEE'S STATE OF DOMICILE, FOR AN
24 INSURER, OR THIS STATE IS THE LICENSEE'S HOME STATE, FOR AN
25 INSURANCE PRODUCER AS THAT TERM IS DEFINED IN SECTION 1201, AND THE
26 CYBERSECURITY EVENT HAS A REASONABLE LIKELIHOOD OF MATERIALLY
27 HARMING EITHER OF THE FOLLOWING:

1 (i) A CONSUMER RESIDING IN THIS STATE.

2 (ii) ANY MATERIAL PART OF A NORMAL OPERATION OF THE LICENSEE.

3 (B) THE LICENSEE REASONABLY BELIEVES THAT THE NONPUBLIC
4 INFORMATION INVOLVED IS OF 250 OR MORE CONSUMERS RESIDING IN THIS
5 STATE AND IS EITHER OF THE FOLLOWING:

6 (i) A CYBERSECURITY EVENT IMPACTING THE LICENSEE OF WHICH
7 NOTICE IS REQUIRED TO BE PROVIDED TO ANY GOVERNMENT BODY, SELF-
8 REGULATORY AGENCY, OR OTHER SUPERVISORY BODY UNDER ANY STATE OR
9 FEDERAL LAW.

10 (ii) A CYBERSECURITY EVENT THAT HAS A REASONABLE LIKELIHOOD OF
11 MATERIALLY HARMING EITHER OF THE FOLLOWING:

12 (A) ANY CONSUMER RESIDING IN THIS STATE.

13 (B) ANY MATERIAL PART OF THE NORMAL OPERATION OF THE LICENSEE.

14 (2) THE LICENSEE SHALL PROVIDE THE INFORMATION UNDER THIS
15 SUBSECTION IN ELECTRONIC FORM AS DIRECTED BY THE DIRECTOR. THE
16 LICENSEE HAS A CONTINUING OBLIGATION TO UPDATE AND SUPPLEMENT
17 INITIAL AND SUBSEQUENT NOTIFICATIONS TO THE DIRECTOR REGARDING
18 MATERIAL CHANGES TO PREVIOUSLY PROVIDED INFORMATION RELATING TO THE
19 CYBERSECURITY EVENT. THE LICENSEE SHALL PROVIDE AS MUCH OF THE
20 FOLLOWING INFORMATION AS POSSIBLE:

21 (A) THE DATE OF THE CYBERSECURITY EVENT.

22 (B) A DESCRIPTION OF HOW THE INFORMATION WAS EXPOSED, LOST,
23 STOLEN, OR BREACHED, INCLUDING THE SPECIFIC ROLES AND
24 RESPONSIBILITIES OF THIRD-PARTY SERVICE PROVIDERS, IF ANY.

25 (C) HOW THE CYBERSECURITY EVENT WAS DISCOVERED.

26 (D) WHETHER ANY LOST, STOLEN, OR BREACHED INFORMATION HAS BEEN
27 RECOVERED AND, IF SO, HOW THIS WAS DONE.

1 (E) THE IDENTITY OF THE SOURCE OF THE CYBERSECURITY EVENT.

2 (F) WHETHER THE LICENSEE HAS FILED A POLICE REPORT OR HAS
3 NOTIFIED ANY REGULATORY, GOVERNMENT, OR LAW ENFORCEMENT AGENCIES
4 AND, IF SO, WHEN THE NOTIFICATION WAS PROVIDED.

5 (G) A DESCRIPTION OF THE SPECIFIC TYPES OF INFORMATION
6 ACQUIRED WITHOUT AUTHORIZATION. AS USED IN THIS SUBDIVISION,
7 "SPECIFIC TYPES OF INFORMATION" MEANS PARTICULAR DATA ELEMENTS
8 INCLUDING, FOR EXAMPLE, TYPES OF MEDICAL INFORMATION, TYPES OF
9 FINANCIAL INFORMATION, OR TYPES OF INFORMATION ALLOWING
10 IDENTIFICATION OF THE CONSUMER.

11 (H) THE PERIOD DURING WHICH THE INFORMATION SYSTEM WAS
12 COMPROMISED BY THE CYBERSECURITY EVENT.

13 (I) THE NUMBER OF TOTAL CONSUMERS IN THIS STATE AFFECTED BY
14 THE CYBERSECURITY EVENT. THE LICENSEE SHALL PROVIDE THE BEST
15 ESTIMATE IN THE INITIAL REPORT TO THE DIRECTOR AND UPDATE THIS
16 ESTIMATE WITH EACH SUBSEQUENT REPORT TO THE DIRECTOR UNDER THIS
17 SECTION.

18 (J) THE RESULTS OF ANY INTERNAL REVIEW IDENTIFYING A LAPSE IN
19 EITHER AUTOMATED CONTROLS OR INTERNAL PROCEDURES, OR CONFIRMING
20 THAT ALL AUTOMATED CONTROLS OR INTERNAL PROCEDURES WERE FOLLOWED.

21 (K) A DESCRIPTION OF EFFORTS BEING UNDERTAKEN TO REMEDIATE THE
22 SITUATION THAT PERMITTED THE CYBERSECURITY EVENT TO OCCUR.

23 (L) A COPY OF THE LICENSEE'S PRIVACY POLICY AND A STATEMENT
24 OUTLINING THE STEPS THE LICENSEE WILL TAKE TO INVESTIGATE AND
25 NOTIFY CONSUMERS AFFECTED BY THE CYBERSECURITY EVENT.

26 (M) THE NAME OF A CONTACT PERSON WHO IS BOTH FAMILIAR WITH THE
27 CYBERSECURITY EVENT AND AUTHORIZED TO ACT FOR THE LICENSEE.

1 (3) FOR A CYBERSECURITY EVENT IN A SYSTEM MAINTAINED BY A
2 THIRD-PARTY SERVICE PROVIDER, OF WHICH THE LICENSEE HAS BECOME
3 AWARE, THE LICENSEE SHALL TREAT THE EVENT AS IT WOULD UNDER THIS
4 SECTION UNLESS THE THIRD-PARTY SERVICE PROVIDER PROVIDES THE NOTICE
5 REQUIRED UNDER THIS SECTION TO THE DIRECTOR. THE COMPUTATION OF THE
6 LICENSEE'S DEADLINES BEGINS ON THE DAY AFTER THE THIRD-PARTY
7 SERVICE PROVIDER NOTIFIES THE LICENSEE OF THE CYBERSECURITY EVENT
8 OR THE LICENSEE OTHERWISE HAS ACTUAL KNOWLEDGE OF THE CYBERSECURITY
9 EVENT, WHICHEVER IS EARLIER. THIS CHAPTER DOES NOT PREVENT OR
10 ABROGATE AN AGREEMENT BETWEEN A LICENSEE AND ANOTHER LICENSEE, A
11 THIRD-PARTY SERVICE PROVIDER, OR ANY OTHER PARTY TO FULFILL ANY OF
12 THE INVESTIGATION REQUIREMENTS IMPOSED UNDER SECTION 557 OR NOTICE
13 REQUIREMENTS IMPOSED UNDER THIS SECTION.

14 (4) FOR A CYBERSECURITY EVENT INVOLVING NONPUBLIC INFORMATION
15 THAT IS USED BY THE LICENSEE THAT IS ACTING AS AN ASSUMING INSURER
16 OR IN THE POSSESSION, CUSTODY, OR CONTROL OF A LICENSEE THAT IS
17 ACTING AS AN ASSUMING INSURER AND THAT DOES NOT HAVE A DIRECT
18 CONTRACTUAL RELATIONSHIP WITH THE AFFECTED CONSUMERS, THE ASSUMING
19 INSURER SHALL NOTIFY ITS AFFECTED CEDING INSURERS AND THE DIRECTOR
20 OF ITS STATE OF DOMICILE WITHIN 10 BUSINESS DAYS AFTER MAKING THE
21 DETERMINATION THAT A CYBERSECURITY EVENT HAS OCCURRED. THE CEDING
22 INSURERS THAT HAVE A DIRECT CONTRACTUAL RELATIONSHIP WITH AFFECTED
23 CONSUMERS SHALL FULFILL THE CONSUMER NOTIFICATION REQUIREMENTS
24 IMPOSED UNDER THIS SECTION. FOR A CYBERSECURITY EVENT INVOLVING
25 NONPUBLIC INFORMATION THAT IS IN THE POSSESSION, CUSTODY, OR
26 CONTROL OF A THIRD-PARTY SERVICE PROVIDER OF A LICENSEE THAT IS AN
27 ASSUMING INSURER, THE ASSUMING INSURER SHALL NOTIFY ITS AFFECTED

1 CEDING INSURERS AND THE DIRECTOR OF ITS STATE OF DOMICILE WITHIN 10
2 BUSINESS DAYS AFTER RECEIVING NOTICE FROM ITS THIRD-PARTY SERVICE
3 PROVIDER THAT A CYBERSECURITY EVENT HAS OCCURRED. THE CEDING
4 INSURERS THAT HAVE A DIRECT CONTRACTUAL RELATIONSHIP WITH AFFECTED
5 CONSUMERS SHALL FULFILL THE CONSUMER NOTIFICATION REQUIREMENTS
6 IMPOSED UNDER THIS CHAPTER.

7 (5) A LICENSEE ACTING AS AN ASSUMING INSURER DOES NOT HAVE
8 OTHER NOTICE OBLIGATIONS RELATING TO A CYBERSECURITY EVENT OR OTHER
9 DATA BREACH UNDER THIS SECTION OR ANY OTHER LAW OF THIS STATE.

10 (6) FOR A CYBERSECURITY EVENT INVOLVING NONPUBLIC INFORMATION
11 THAT IS IN THE POSSESSION, CUSTODY, OR CONTROL OF A LICENSEE THAT
12 IS AN INSURER OR ITS THIRD-PARTY SERVICE PROVIDER FOR WHICH A
13 CONSUMER ACCESSED THE INSURER'S SERVICES THROUGH AN INDEPENDENT
14 INSURANCE PRODUCER, AND FOR WHICH CONSUMER NOTICE IS REQUIRED UNDER
15 THIS CHAPTER, THE INSURER SHALL NOTIFY THE PRODUCERS OF RECORD OF
16 ALL AFFECTED CONSUMERS OF THE CYBERSECURITY EVENT NOT LATER THAN
17 THE TIME AT WHICH NOTICE IS PROVIDED TO THE AFFECTED CONSUMERS. THE
18 INSURER IS EXCUSED FROM THIS OBLIGATION FOR ANY PRODUCER WHO IS NOT
19 AUTHORIZED BY LAW OR CONTRACT TO SELL, SOLICIT, OR NEGOTIATE ON
20 BEHALF OF THE INSURER, AND IN THOSE INSTANCES IN WHICH THE INSURER
21 DOES NOT HAVE THE CURRENT PRODUCER OF RECORD INFORMATION FOR ANY
22 INDIVIDUAL CONSUMER.

23 SEC. 561. (1) UNLESS THE LICENSEE DETERMINES THAT THE SECURITY
24 BREACH HAS NOT OR IS NOT LIKELY TO CAUSE SUBSTANTIAL LOSS OR INJURY
25 TO, OR RESULT IN IDENTITY THEFT WITH RESPECT TO, 1 OR MORE
26 RESIDENTS OF THIS STATE, A LICENSEE THAT OWNS OR LICENSES DATA THAT
27 ARE INCLUDED IN A DATABASE THAT DISCOVERS A SECURITY BREACH, OR

1 RECEIVES NOTICE OF A SECURITY BREACH UNDER SUBSECTION (2), SHALL
2 PROVIDE A NOTICE OF THE SECURITY BREACH TO EACH RESIDENT OF THIS
3 STATE WHO MEETS 1 OR MORE OF THE FOLLOWING:

4 (A) THAT RESIDENT'S UNENCRYPTED AND UNREDACTED PERSONAL
5 INFORMATION WAS ACCESSED AND ACQUIRED BY AN UNAUTHORIZED PERSON.

6 (B) THAT RESIDENT'S PERSONAL INFORMATION WAS ACCESSED AND
7 ACQUIRED IN ENCRYPTED FORM BY A LICENSEE WITH UNAUTHORIZED ACCESS
8 TO THE ENCRYPTION KEY.

9 (2) UNLESS THE LICENSEE DETERMINES THAT THE SECURITY BREACH
10 HAS NOT OR IS NOT LIKELY TO CAUSE SUBSTANTIAL LOSS OR INJURY TO, OR
11 RESULT IN IDENTITY THEFT WITH RESPECT TO, 1 OR MORE RESIDENTS OF
12 THIS STATE, A LICENSEE THAT MAINTAINS A DATABASE THAT INCLUDES DATA
13 THAT THE LICENSEE DOES NOT OWN OR LICENSE THAT DISCOVERS A BREACH
14 OF THE SECURITY OF THE DATABASE SHALL PROVIDE A NOTICE TO THE OWNER
15 OR LICENSOR OF THE INFORMATION OF THE SECURITY BREACH.

16 (3) IN DETERMINING WHETHER A SECURITY BREACH IS NOT LIKELY TO
17 CAUSE SUBSTANTIAL LOSS OR INJURY TO, OR RESULT IN IDENTITY THEFT
18 WITH RESPECT TO, 1 OR MORE RESIDENTS OF THIS STATE UNDER SUBSECTION
19 (1) OR (2), A LICENSEE SHALL ACT WITH THE CARE AN ORDINARILY
20 PRUDENT PERSON OR AGENCY IN LIKE POSITION WOULD EXERCISE UNDER
21 SIMILAR CIRCUMSTANCES.

22 (4) A LICENSEE SHALL PROVIDE ANY NOTICE REQUIRED UNDER THIS
23 SECTION WITHOUT UNREASONABLE DELAY. A LICENSEE MAY DELAY PROVIDING
24 NOTICE WITHOUT VIOLATING THIS SUBSECTION IF EITHER OF THE FOLLOWING
25 IS MET:

26 (A) A DELAY IS NECESSARY IN ORDER FOR THE LICENSEE TO TAKE ANY
27 MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE SECURITY BREACH

1 AND RESTORE THE REASONABLE INTEGRITY OF THE DATABASE. HOWEVER, THE
2 LICENSEE SHALL PROVIDE THE NOTICE REQUIRED UNDER THIS SUBSECTION
3 WITHOUT UNREASONABLE DELAY AFTER THE LICENSEE COMPLETES THE
4 MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE SECURITY BREACH
5 AND RESTORE THE REASONABLE INTEGRITY OF THE DATABASE.

6 (B) A LAW ENFORCEMENT AGENCY DETERMINES AND ADVISES THE
7 LICENSEE THAT PROVIDING A NOTICE WILL IMPEDE A CRIMINAL OR CIVIL
8 INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY. HOWEVER,
9 THE LICENSEE SHALL PROVIDE THE NOTICE REQUIRED UNDER THIS SECTION
10 WITHOUT UNREASONABLE DELAY AFTER THE LAW ENFORCEMENT AGENCY
11 DETERMINES THAT PROVIDING THE NOTICE WILL NO LONGER IMPEDE THE
12 INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY.

13 (5) A LICENSEE SHALL PROVIDE ANY NOTICE REQUIRED UNDER THIS
14 SECTION BY PROVIDING 1 OR MORE OF THE FOLLOWING TO THE RECIPIENT:

15 (A) WRITTEN NOTICE SENT TO THE RECIPIENT AT THE RECIPIENT'S
16 POSTAL ADDRESS IN THE RECORDS OF THE LICENSEE.

17 (B) WRITTEN NOTICE SENT ELECTRONICALLY TO THE RECIPIENT IF ANY
18 OF THE FOLLOWING ARE MET:

19 (i) THE RECIPIENT HAS EXPRESSLY CONSENTED TO RECEIVE
20 ELECTRONIC NOTICE.

21 (ii) THE LICENSEE HAS AN EXISTING BUSINESS RELATIONSHIP WITH
22 THE RECIPIENT THAT INCLUDES PERIODIC ELECTRONIC MAIL COMMUNICATIONS
23 AND BASED ON THOSE COMMUNICATIONS THE LICENSEE REASONABLY BELIEVES
24 THAT IT HAS THE RECIPIENT'S CURRENT ELECTRONIC MAIL ADDRESS.

25 (iii) THE LICENSEE CONDUCTS ITS BUSINESS PRIMARILY THROUGH
26 INTERNET ACCOUNT TRANSACTIONS OR ON THE INTERNET.

27 (C) IF NOT OTHERWISE PROHIBITED BY STATE OR FEDERAL LAW,

1 NOTICE GIVEN BY TELEPHONE BY AN INDIVIDUAL WHO REPRESENTS THE
2 LICENSEE IF ALL OF THE FOLLOWING ARE MET:

3 (i) THE NOTICE IS NOT GIVEN IN WHOLE OR IN PART BY USE OF A
4 RECORDED MESSAGE.

5 (ii) THE RECIPIENT HAS EXPRESSLY CONSENTED TO RECEIVE NOTICE
6 BY TELEPHONE, OR IF THE RECIPIENT HAS NOT EXPRESSLY CONSENTED TO
7 RECEIVE NOTICE BY TELEPHONE, THE LICENSEE ALSO PROVIDES NOTICE
8 UNDER SUBDIVISION (A) OR (B) IF THE NOTICE BY TELEPHONE DOES NOT
9 RESULT IN A LIVE CONVERSATION BETWEEN THE INDIVIDUAL REPRESENTING
10 THE LICENSEE AND THE RECIPIENT WITHIN 3 BUSINESS DAYS AFTER THE
11 INITIAL ATTEMPT TO PROVIDE TELEPHONIC NOTICE.

12 (D) SUBSTITUTE NOTICE, IF THE LICENSEE DEMONSTRATES THAT THE
13 COST OF PROVIDING NOTICE UNDER SUBDIVISION (A), (B), OR (C) WILL
14 EXCEED \$250,000.00 OR THAT THE LICENSEE HAS TO PROVIDE NOTICE TO
15 MORE THAN 500,000 RESIDENTS OF THIS STATE. A LICENSEE PROVIDES
16 SUBSTITUTE NOTICE UNDER THIS SUBDIVISION BY DOING ALL OF THE
17 FOLLOWING:

18 (i) IF THE LICENSEE HAS ELECTRONIC MAIL ADDRESSES FOR ANY OF
19 THE RESIDENTS OF THIS STATE WHO ARE ENTITLED TO RECEIVE THE NOTICE,
20 PROVIDING ELECTRONIC NOTICE TO THOSE RESIDENTS.

21 (ii) IF THE LICENSEE MAINTAINS A WEBSITE, CONSPICUOUSLY
22 POSTING THE NOTICE ON THAT WEBSITE.

23 (iii) NOTIFYING MAJOR STATEWIDE MEDIA. A NOTIFICATION UNDER
24 THIS SUBPARAGRAPH MUST INCLUDE A TELEPHONE NUMBER OR A WEBSITE
25 ADDRESS THAT A PERSON MAY USE TO OBTAIN ADDITIONAL ASSISTANCE AND
26 INFORMATION.

27 (6) A NOTICE UNDER THIS SECTION MUST DO ALL OF THE FOLLOWING:

1 (A) FOR A NOTICE PROVIDED UNDER SUBSECTION (5) (A) OR (B), BE
2 WRITTEN IN A CLEAR AND CONSPICUOUS MANNER AND CONTAIN THE CONTENT
3 REQUIRED UNDER SUBDIVISIONS (C) TO (G).

4 (B) FOR A NOTICE PROVIDED UNDER SUBSECTION (5) (C), CLEARLY
5 COMMUNICATE THE CONTENT REQUIRED UNDER SUBDIVISIONS (C) TO (G) TO
6 THE RECIPIENT OF THE TELEPHONE CALL.

7 (C) DESCRIBE THE SECURITY BREACH IN GENERAL TERMS.

8 (D) DESCRIBE THE TYPE OF PERSONAL INFORMATION THAT IS THE
9 SUBJECT OF THE UNAUTHORIZED ACCESS OR USE.

10 (E) IF APPLICABLE, GENERALLY DESCRIBE WHAT THE LICENSEE
11 PROVIDING THE NOTICE HAS DONE TO PROTECT DATA FROM FURTHER SECURITY
12 BREACHES.

13 (F) INCLUDE A TELEPHONE NUMBER WHERE A NOTICE RECIPIENT MAY
14 OBTAIN ASSISTANCE OR ADDITIONAL INFORMATION.

15 (G) REMIND NOTICE RECIPIENTS OF THE NEED TO REMAIN VIGILANT
16 FOR INCIDENTS OF FRAUD AND IDENTITY THEFT.

17 (7) A LICENSEE MAY PROVIDE ANY NOTICE REQUIRED UNDER THIS
18 SECTION UNDER AN AGREEMENT BETWEEN THE LICENSEE AND ANOTHER
19 LICENSEE, IF THE NOTICE PROVIDED UNDER THE AGREEMENT DOES NOT
20 CONFLICT WITH THIS SECTION.

21 (8) EXCEPT AS PROVIDED IN THIS SUBSECTION, AFTER A LICENSEE
22 PROVIDES A NOTICE UNDER THIS SECTION, THE LICENSEE SHALL NOTIFY
23 EACH CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON
24 CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED IN 15 USC 1681A(P), OF
25 THE SECURITY BREACH WITHOUT UNREASONABLE DELAY. A NOTIFICATION
26 UNDER THIS SUBSECTION MUST INCLUDE THE NUMBER OF NOTICES THAT THE
27 LICENSEE PROVIDED TO RESIDENTS OF THIS STATE AND THE TIMING OF

1 THOSE NOTICES. THIS SUBSECTION DOES NOT APPLY IF EITHER OF THE
2 FOLLOWING IS MET:

3 (A) THE LICENSEE IS REQUIRED UNDER THIS SECTION TO PROVIDE
4 NOTICE OF A SECURITY BREACH TO 1,000 OR FEWER RESIDENTS OF THIS
5 STATE.

6 (B) THE LICENSEE IS SUBJECT TO 15 USC 6801 TO 6809.

7 (9) A LICENSEE THAT IS SUBJECT TO AND COMPLIES WITH THE HEALTH
8 INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, PUBLIC LAW
9 104-191, AND WITH REGULATIONS PROMULGATED UNDER THAT ACT, 45 CFR
10 PARTS 160 AND 164, FOR THE PREVENTION OF UNAUTHORIZED ACCESS TO
11 CUSTOMER INFORMATION AND CUSTOMER NOTICE IS CONSIDERED TO BE IN
12 COMPLIANCE WITH THIS SECTION.

13 (10) A PERSON THAT PROVIDES NOTICE OF A SECURITY BREACH IN THE
14 MANNER DESCRIBED IN THIS SECTION WHEN A SECURITY BREACH HAS NOT
15 OCCURRED, WITH THE INTENT TO DEFRAUD, IS GUILTY OF A MISDEMEANOR
16 PUNISHABLE AS FOLLOWS:

17 (A) EXCEPT AS OTHERWISE PROVIDED UNDER SUBDIVISIONS (B) AND
18 (C), BY IMPRISONMENT FOR NOT MORE THAN 93 DAYS OR A FINE OF NOT
19 MORE THAN \$250.00 FOR EACH VIOLATION, OR BOTH.

20 (B) FOR A SECOND VIOLATION, BY IMPRISONMENT FOR NOT MORE THAN
21 93 DAYS OR A FINE OF NOT MORE THAN \$500.00 FOR EACH VIOLATION, OR
22 BOTH.

23 (C) FOR A THIRD OR SUBSEQUENT VIOLATION, BY IMPRISONMENT FOR
24 NOT MORE THAN 93 DAYS OR A FINE OF NOT MORE THAN \$750.00 FOR EACH
25 VIOLATION, OR BOTH.

26 (11) SUBJECT TO SUBSECTION (12), A PERSON THAT KNOWINGLY FAILS
27 TO PROVIDE A NOTICE OF A SECURITY BREACH REQUIRED UNDER THIS

1 SECTION MAY BE ORDERED TO PAY A CIVIL FINE OF NOT MORE THAN \$250.00
2 FOR EACH FAILURE TO PROVIDE NOTICE. THE ATTORNEY GENERAL OR A
3 PROSECUTING ATTORNEY MAY BRING AN ACTION TO RECOVER A CIVIL FINE
4 UNDER THIS SECTION.

5 (12) THE AGGREGATE LIABILITY OF A PERSON FOR CIVIL FINES UNDER
6 SUBSECTION (11) FOR MULTIPLE VIOLATIONS OF SUBSECTION (11) THAT
7 ARISE FROM THE SAME SECURITY BREACH MUST NOT EXCEED \$750,000.00.

8 (13) SUBSECTIONS (10) AND (11) DO NOT AFFECT THE AVAILABILITY
9 OF ANY CIVIL REMEDY FOR A VIOLATION OF STATE OR FEDERAL LAW.

10 (14) THIS SECTION APPLIES TO THE DISCOVERY OR NOTIFICATION OF
11 A BREACH OF THE SECURITY OF A DATABASE THAT OCCURS AFTER DECEMBER
12 31, 2019.

13 (15) THIS SECTION DOES NOT APPLY TO THE ACCESS OR ACQUISITION
14 BY A PERSON OR AGENCY OF FEDERAL, STATE, OR LOCAL GOVERNMENT
15 RECORDS OR DOCUMENTS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.

16 (16) THIS SECTION DEALS WITH SUBJECT MATTER THAT IS OF
17 STATEWIDE CONCERN, AND ANY CHARTER, ORDINANCE, RESOLUTION,
18 REGULATION, RULE, OR OTHER ACTION BY A MUNICIPAL CORPORATION OR
19 OTHER POLITICAL SUBDIVISION OF THIS STATE TO REGULATE, DIRECTLY OR
20 INDIRECTLY, ANY MATTER EXPRESSLY SET FORTH IN THIS SECTION IS
21 PREEMPTED.

22 (17) AS USED IN THIS SECTION:

23 (A) "DATA" MEANS THAT TERM AS DEFINED IN SECTION 3 OF THE
24 IDENTITY THEFT PROTECTION ACT, 2004 PA 452, MCL 445.63.

25 (B) "IDENTITY THEFT" MEANS THAT TERM AS DEFINED IN SECTION 3
26 OF THE IDENTITY THEFT PROTECTION ACT, 2004 PA 452, MCL 445.63.

27 (C) "PERSONAL INFORMATION" MEANS THAT TERM AS DEFINED IN

1 SECTION 3 OF THE IDENTITY THEFT PROTECTION ACT, 2004 PA 452, MCL
2 445.63.

3 (D) "SECURITY BREACH" MEANS THAT TERM AS DEFINED IN SECTION 3
4 OF THE IDENTITY THEFT PROTECTION ACT, 2004 PA 452, MCL 445.63.

5 SEC. 563. (1) ANY DOCUMENTS, MATERIALS, OR OTHER INFORMATION
6 IN THE CONTROL OR POSSESSION OF THE DEPARTMENT THAT IS FURNISHED BY
7 A LICENSEE OR AN EMPLOYEE OR AGENT OF THE LICENSEE ACTING ON BEHALF
8 OF THE LICENSEE UNDER SECTION 555(9), SECTION 559(2)(B), (C), (D),
9 (E), (H), (I), AND (J), OR THAT IS OBTAINED BY THE DIRECTOR IN AN
10 INVESTIGATION OR EXAMINATION BY THE DIRECTOR IS CONFIDENTIAL BY LAW
11 AND PRIVILEGED, IS NOT SUBJECT TO THE FREEDOM OF INFORMATION ACT,
12 1976 PA 442, MCL 15.231 TO 15.246, IS NOT SUBJECT TO SUBPOENA, AND
13 IS NOT SUBJECT TO DISCOVERY OR ADMISSIBLE IN EVIDENCE IN ANY
14 PRIVATE CIVIL ACTION. HOWEVER, THE DIRECTOR IS AUTHORIZED TO USE
15 THE DOCUMENTS, MATERIALS, OR OTHER INFORMATION IN THE FURTHERANCE
16 OF ANY REGULATORY OR LEGAL ACTION BROUGHT AS A PART OF THE
17 DIRECTOR'S DUTIES. THE DIRECTOR SHALL NOT OTHERWISE MAKE THE
18 DOCUMENTS, MATERIALS, OR OTHER INFORMATION PUBLIC WITHOUT THE PRIOR
19 WRITTEN CONSENT OF THE LICENSEE.

20 (2) NEITHER THE DIRECTOR NOR ANY PERSON THAT RECEIVED
21 DOCUMENTS, MATERIALS, OR OTHER INFORMATION WHILE ACTING UNDER THE
22 AUTHORITY OF THE DIRECTOR IS PERMITTED OR REQUIRED TO TESTIFY IN
23 ANY PRIVATE CIVIL ACTION CONCERNING ANY CONFIDENTIAL DOCUMENTS,
24 MATERIALS, OR INFORMATION UNDER SUBSECTION (1).

25 (3) TO ASSIST IN THE PERFORMANCE OF THE DIRECTOR'S DUTIES
26 UNDER THIS CHAPTER, THE DIRECTOR MAY DO ANY OF THE FOLLOWING:

27 (A) SHARE DOCUMENTS, MATERIALS, OR OTHER INFORMATION,

1 INCLUDING THE CONFIDENTIAL AND PRIVILEGED DOCUMENTS, MATERIALS, OR
2 INFORMATION SUBJECT TO SUBSECTION (1), WITH OTHER STATE, FEDERAL,
3 AND INTERNATIONAL REGULATORY AGENCIES, WITH THE NATIONAL
4 ASSOCIATION OF INSURANCE COMMISSIONERS, ITS AFFILIATES, OR ITS
5 SUBSIDIARIES, AND WITH STATE, FEDERAL, AND INTERNATIONAL LAW
6 ENFORCEMENT AUTHORITIES, IF THE RECIPIENT AGREES IN WRITING TO
7 MAINTAIN THE CONFIDENTIALITY AND PRIVILEGED STATUS OF THE DOCUMENT,
8 MATERIAL, OR OTHER INFORMATION.

9 (B) RECEIVE DOCUMENTS, MATERIALS, OR INFORMATION, INCLUDING
10 OTHERWISE CONFIDENTIAL AND PRIVILEGED DOCUMENTS, MATERIALS, OR
11 INFORMATION, FROM THE NATIONAL ASSOCIATION OF INSURANCE
12 COMMISSIONERS, ITS AFFILIATES, OR ITS SUBSIDIARIES, AND FROM
13 REGULATORY AND LAW ENFORCEMENT OFFICIALS OF OTHER FOREIGN OR
14 DOMESTIC JURISDICTIONS, AND SHALL MAINTAIN AS CONFIDENTIAL OR
15 PRIVILEGED ANY DOCUMENT, MATERIAL, OR INFORMATION RECEIVED WITH
16 NOTICE OR THE UNDERSTANDING THAT IT IS CONFIDENTIAL OR PRIVILEGED
17 UNDER THE LAWS OF THE JURISDICTION THAT IS THE SOURCE OF THE
18 DOCUMENT, MATERIAL, OR INFORMATION.

19 (C) SHARE DOCUMENTS, MATERIALS, OR OTHER INFORMATION SUBJECT
20 TO SUBSECTION (1) WITH A THIRD-PARTY CONSULTANT OR VENDOR IF THE
21 CONSULTANT AGREES IN WRITING TO MAINTAIN THE CONFIDENTIALITY AND
22 PRIVILEGED STATUS OF THE DOCUMENT, MATERIAL, OR OTHER INFORMATION.

23 (D) ENTER INTO AGREEMENTS GOVERNING SHARING AND USE OF
24 INFORMATION CONSISTENT WITH THIS SUBSECTION.

25 (4) A WAIVER OF ANY APPLICABLE PRIVILEGE OR CLAIM OF
26 CONFIDENTIALITY IN THE DOCUMENTS, MATERIALS, OR INFORMATION DOES
27 NOT OCCUR AS A RESULT OF DISCLOSURE TO THE DIRECTOR UNDER THIS

1 SECTION OR AS A RESULT OF SHARING AS AUTHORIZED UNDER SUBSECTION
2 (3) .

3 (5) THIS CHAPTER DOES NOT PROHIBIT THE DIRECTOR FROM RELEASING
4 FINAL, ADJUDICATED ACTIONS THAT ARE OPEN TO PUBLIC INSPECTION
5 PURSUANT TO THE FREEDOM OF INFORMATION ACT, 1976 PA 442, MCL 15.231
6 TO 15.246, TO A DATABASE OR OTHER CLEARINGHOUSE SERVICE MAINTAINED
7 BY THE NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, ITS
8 AFFILIATES, OR ITS SUBSIDIARIES.

9 (6) ANY DOCUMENTS, MATERIALS, OR OTHER INFORMATION IN THE
10 POSSESSION OR CONTROL OF THE NATIONAL ASSOCIATION OF INSURANCE
11 COMMISSIONERS OR A THIRD-PARTY CONSULTANT OR VENDOR UNDER THIS
12 CHAPTER IS CONFIDENTIAL BY LAW AND PRIVILEGED, IS NOT SUBJECT TO
13 THE FREEDOM OF INFORMATION ACT, 1976 PA 442, MCL 15.231 TO 15.246,
14 IS NOT SUBJECT TO SUBPOENA, AND IS NOT SUBJECT TO DISCOVERY OR
15 ADMISSIBLE IN EVIDENCE IN ANY PRIVATE CIVIL ACTION.

16 SEC. 565. (1) A LICENSEE THAT MEETS ANY OF THE FOLLOWING
17 CRITERIA IS EXEMPT FROM SECTION 555:

18 (A) THE LICENSEE HAS FEWER THAN 50 EMPLOYEES, INCLUDING ANY
19 INDEPENDENT CONTRACTORS.

20 (B) THE LICENSEE HAS LESS THAN \$10,000,000.00 IN GROSS ANNUAL
21 REVENUE.

22 (C) THE LICENSEE HAS LESS THAN \$25,000,000.00 IN YEAR-END
23 TOTAL ASSETS.

24 (2) A LICENSEE SUBJECT TO AND IN COMPLIANCE WITH THE HEALTH
25 INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, PUBLIC LAW
26 104-191, AND WITH REGULATIONS PROMULGATED UNDER THAT ACT, IS NOT
27 REQUIRED TO COMPLY WITH THIS CHAPTER EXCEPT FOR THE REQUIREMENTS

1 UNDER SECTIONS 559 AND 561.

2 (3) AN EMPLOYEE, AGENT, REPRESENTATIVE, OR DESIGNEE OF A
3 LICENSEE, WHO IS ALSO A LICENSEE, IS EXEMPT FROM SECTION 555 AND
4 DOES NOT NEED TO DEVELOP ITS OWN INFORMATION SECURITY PROGRAM TO
5 THE EXTENT THAT THE EMPLOYEE, AGENT, REPRESENTATIVE, OR DESIGNEE IS
6 COVERED BY THE INFORMATION SECURITY PROGRAM OF THE OTHER LICENSEE.

7 (4) IF A LICENSEE CEASES TO QUALIFY FOR AN EXCEPTION UNDER
8 SUBSECTION (1), THE LICENSEE HAS 180 DAYS TO COMPLY WITH THIS
9 CHAPTER.

10 (5) THIS CHAPTER TAKES EFFECT ON JANUARY 20, 2020. A LICENSEE
11 SHALL IMPLEMENT SECTION 555 BY JANUARY 20, 2021. HOWEVER, A
12 LICENSEE HAS UNTIL JANUARY 20, 2022 TO IMPLEMENT SECTION 555(6).