

SUBSTITUTE FOR
HOUSE BILL NO. 6491

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:

1
2
3
4
5
6
7
8
9

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, FOR THIS
STATE, APPLICABLE TO LICENSEES FOR DATA SECURITY, THE INVESTIGATION
OF A CYBERSECURITY EVENT, AND NOTIFICATION TO THE DIRECTOR.

SEC. 553. AS USED IN THIS CHAPTER:

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

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

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

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

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

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

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

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

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

1 (E) "INFORMATION SECURITY PROGRAM" MEANS THE ADMINISTRATIVE,
2 TECHNICAL, AND PHYSICAL SAFEGUARDS THAT A LICENSEE USES TO ACCESS,
3 COLLECT, DISTRIBUTE, PROCESS, PROTECT, STORE, USE, TRANSMIT,
4 DISPOSE OF, OR OTHERWISE HANDLE NONPUBLIC INFORMATION.

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

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

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

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

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

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

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

1 FOLLOWING:

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

6 (A) SOCIAL SECURITY NUMBER.

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

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

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

12 (E) BIOMETRIC RECORDS.

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

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

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

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

22 (J) "PUBLICLY AVAILABLE INFORMATION" MEANS ANY INFORMATION
23 THAT A LICENSEE HAS A REASONABLE BASIS TO BELIEVE IS LAWFULLY MADE
24 AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL
25 GOVERNMENT RECORDS, BY WIDELY DISTRIBUTED MEDIA, OR BY DISCLOSURES
26 TO THE GENERAL PUBLIC THAT ARE REQUIRED TO BE MADE BY FEDERAL,
27 STATE, OR LOCAL LAW. A LICENSEE HAS A REASONABLE BASIS TO BELIEVE

1 THAT INFORMATION IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC
2 IF BOTH OF THE FOLLOWING APPLY:

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

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

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

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

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

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

27 (A) PROTECT THE SECURITY AND CONFIDENTIALITY OF NONPUBLIC

1 INFORMATION AND THE SECURITY OF THE INFORMATION SYSTEM.

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

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

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

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

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

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

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

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

27 (i) EMPLOYEE TRAINING AND MANAGEMENT.

1 (ii) INFORMATION SYSTEMS, INCLUDING NETWORK AND SOFTWARE
2 DESIGN, AS WELL AS INFORMATION CLASSIFICATION, GOVERNANCE,
3 PROCESSING, STORAGE, TRANSMISSION, AND DISPOSAL.

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

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

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

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

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

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

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

1 (iii) RESTRICTING PHYSICAL ACCESS TO NONPUBLIC INFORMATION TO
2 AUTHORIZED INDIVIDUALS ONLY.

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

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

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

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

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

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

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

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

27 (C) INCLUDE CYBERSECURITY RISKS IN THE LICENSEE'S ENTERPRISE

1 RISK MANAGEMENT PROCESS.

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

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

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

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

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

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

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

26 (iii) IF EXECUTIVE MANAGEMENT DELEGATES ANY OF ITS
27 RESPONSIBILITIES UNDER THIS SECTION, IT SHALL OVERSEE THE

1 DEVELOPMENT, IMPLEMENTATION, AND MAINTENANCE OF THE LICENSEE'S
2 INFORMATION SECURITY PROGRAM PREPARED BY A DELEGATE AND SHALL
3 RECEIVE A REPORT FROM THE DELEGATE COMPLYING WITH THE REQUIREMENTS
4 OF THE REPORT TO THE BOARD OF DIRECTORS.

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

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

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

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

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

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

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

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

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

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

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

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

1 LICENSEE, SHALL CONDUCT A PROMPT INVESTIGATION.

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

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

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

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

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

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

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

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

1 HARMING EITHER OF THE FOLLOWING:

2 (i) A CONSUMER RESIDING IN THIS STATE.

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

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

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

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

13 (A) ANY CONSUMER RESIDING IN THIS STATE.

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

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

22 (A) THE DATE OF THE CYBERSECURITY EVENT.

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

26 (C) HOW THE CYBERSECURITY EVENT WAS DISCOVERED.

27 (D) WHETHER ANY LOST, STOLEN, OR BREACHED INFORMATION HAS BEEN

1 RECOVERED AND, IF SO, HOW THIS WAS DONE.

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

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

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

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

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

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

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

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

27 (M) THE NAME OF A CONTACT PERSON WHO IS BOTH FAMILIAR WITH THE

1 CYBERSECURITY EVENT AND AUTHORIZED TO ACT FOR THE LICENSEE.

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

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

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

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

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

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

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

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

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

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

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

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

27 (A) A DELAY IS NECESSARY IN ORDER FOR THE LICENSEE TO TAKE ANY

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

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

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

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

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

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

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

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

1 (C) IF NOT OTHERWISE PROHIBITED BY STATE OR FEDERAL LAW,
2 NOTICE GIVEN BY TELEPHONE BY AN INDIVIDUAL WHO REPRESENTS THE
3 LICENSEE IF ALL OF THE FOLLOWING ARE MET:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 LICENSEE PROVIDED TO RESIDENTS OF THIS STATE AND THE TIMING OF
2 THOSE NOTICES. THIS SUBSECTION DOES NOT APPLY IF EITHER OF THE
3 FOLLOWING IS MET:

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

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

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

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

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

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

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

27 (11) SUBJECT TO SUBSECTION (12), A PERSON THAT KNOWINGLY FAILS

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

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

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

11 (14) THIS SECTION APPLIES TO THE DISCOVERY OR NOTIFICATION OF
12 A BREACH OF THE SECURITY OF A DATABASE THAT OCCURS AFTER DECEMBER
13 31, 2019.

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

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

23 (17) AS USED IN THIS SECTION:

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

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

1 (C) "PERSONAL INFORMATION" MEANS THAT TERM AS DEFINED IN
2 SECTION 3 OF THE IDENTITY THEFT PROTECTION ACT, 2004 PA 452, MCL
3 445.63.

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

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

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

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

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

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

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

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

26 (4) A WAIVER OF ANY APPLICABLE PRIVILEGE OR CLAIM OF
27 CONFIDENTIALITY IN THE DOCUMENTS, MATERIALS, OR INFORMATION DOES

1 NOT OCCUR AS A RESULT OF DISCLOSURE TO THE DIRECTOR UNDER THIS
2 SECTION OR AS A RESULT OF SHARING AS AUTHORIZED UNDER SUBSECTION
3 (3) .

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

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

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

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

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

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

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

1 REQUIRED TO COMPLY WITH THIS CHAPTER EXCEPT FOR THE REQUIREMENTS
2 UNDER SECTIONS 559 AND 561.

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

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

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