

SENATE 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.

1 SEC. 553. AS USED IN THIS CHAPTER:

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

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

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

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

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

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

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

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

26 (E) "INFORMATION SECURITY PROGRAM" MEANS THE ADMINISTRATIVE,
27 TECHNICAL, AND PHYSICAL SAFEGUARDS THAT A LICENSEE USES TO ACCESS,

1 COLLECT, DISTRIBUTE, PROCESS, PROTECT, STORE, USE, TRANSMIT,
2 DISPOSE OF, OR OTHERWISE HANDLE NONPUBLIC INFORMATION.

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

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

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

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

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

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

24 (I) "NONPUBLIC INFORMATION" MEANS ELECTRONIC INFORMATION THAT
25 IS NOT PUBLICLY AVAILABLE INFORMATION AND IS ANY OF THE FOLLOWING:

26 (i) BUSINESS-RELATED INFORMATION OF A LICENSEE, THE TAMPERING
27 WITH WHICH, OR UNAUTHORIZED DISCLOSURE, ACCESS, OR USE OF WHICH,

1 WOULD CAUSE A MATERIAL ADVERSE IMPACT TO THE BUSINESS, OPERATIONS,
2 OR SECURITY OF THE LICENSEE.

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

7 (A) SOCIAL SECURITY NUMBER.

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

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

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

13 (E) BIOMETRIC RECORDS.

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

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

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

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

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

1 STATE, OR LOCAL LAW. A LICENSEE HAS A REASONABLE BASIS TO BELIEVE
2 THAT INFORMATION IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC
3 IF BOTH OF THE FOLLOWING APPLY:

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

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

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

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

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

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

1 (A) PROTECT THE SECURITY AND CONFIDENTIALITY OF NONPUBLIC
2 INFORMATION AND THE SECURITY OF THE INFORMATION SYSTEM.

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

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

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

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

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

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

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

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

1 (i) EMPLOYEE TRAINING AND MANAGEMENT.

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

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

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

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

13 (A) DESIGN ITS INFORMATION SECURITY PROGRAM TO MITIGATE THE
14 IDENTIFIED RISKS, 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.

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

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

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

1 BUSINESS OBJECTIVES AND THE ORGANIZATION'S RISK STRATEGY.

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

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

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

10 (vi) ADDING PROCEDURES FOR EVALUATING, ASSESSING, OR TESTING
11 THE SECURITY OF EXTERNALLY DEVELOPED APPLICATIONS USED BY THE
12 LICENSEE.

13 (vii) MODIFYING THE INFORMATION SYSTEM IN ACCORDANCE WITH THE
14 LICENSEE'S INFORMATION SECURITY PROGRAM.

15 (viii) USING EFFECTIVE CONTROLS, WHICH MAY INCLUDE MULTI-
16 FACTOR AUTHENTICATION PROCEDURES FOR EMPLOYEES ACCESSING NONPUBLIC
17 INFORMATION.

18 (ix) REGULARLY TESTING AND MONITORING SYSTEMS AND PROCEDURES
19 TO DETECT ACTUAL AND ATTEMPTED ATTACKS ON, OR INTRUSIONS INTO,
20 INFORMATION SYSTEMS.

21 (x) INCLUDING AUDIT TRAILS WITHIN THE INFORMATION SECURITY
22 PROGRAM DESIGNED TO DETECT AND RESPOND TO CYBERSECURITY EVENTS AND
23 DESIGNED TO RECONSTRUCT MATERIAL FINANCIAL TRANSACTIONS SUFFICIENT
24 TO SUPPORT NORMAL OPERATIONS AND OBLIGATIONS OF THE LICENSEE.

25 (xi) IMPLEMENTING MEASURES TO PROTECT AGAINST DESTRUCTION,
26 LOSS, OR DAMAGE OF NONPUBLIC INFORMATION DUE TO ENVIRONMENTAL
27 HAZARDS, SUCH AS FIRE AND WATER DAMAGE OR OTHER CATASTROPHES OR

1 TECHNOLOGICAL FAILURES.

2 (xii) DEVELOPING, IMPLEMENTING, AND MAINTAINING PROCEDURES FOR
3 THE SECURE DISPOSAL OF NONPUBLIC INFORMATION IN ANY FORMAT.

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

6 (D) STAY INFORMED REGARDING EMERGING THREATS OR
7 VULNERABILITIES AND UTILIZE REASONABLE SECURITY MEASURES WHEN
8 SHARING INFORMATION RELATIVE TO THE CHARACTER OF THE SHARING AND
9 THE TYPE OF INFORMATION SHARED.

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

13 (5) IF A LICENSEE HAS A BOARD OF DIRECTORS, THE BOARD OR AN
14 APPROPRIATE COMMITTEE OF THE BOARD SHALL, AT A MINIMUM, DO ALL OF
15 THE FOLLOWING:

16 (A) REQUIRE THE LICENSEE'S EXECUTIVE MANAGEMENT OR ITS
17 DELEGATES TO DEVELOP, IMPLEMENT, AND MAINTAIN THE LICENSEE'S
18 INFORMATION SECURITY PROGRAM.

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

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

24 (ii) MATERIAL MATTERS RELATED TO THE INFORMATION SECURITY
25 PROGRAM, ADDRESSING ISSUES SUCH AS RISK ASSESSMENT, RISK MANAGEMENT
26 AND CONTROL DECISIONS, RESULTS OF TESTING, CYBERSECURITY EVENTS OR
27 VIOLATIONS, AND MANAGEMENT'S RESPONSES TO THE MATERIAL MATTERS

1 DESCRIBED IN THIS SUBPARAGRAPH, AND RECOMMENDATIONS FOR CHANGES IN
2 THE INFORMATION SECURITY PROGRAM.

3 (iii) IF EXECUTIVE MANAGEMENT DELEGATES ANY OF ITS
4 RESPONSIBILITIES UNDER THIS SECTION, IT SHALL OVERSEE THE
5 DEVELOPMENT, IMPLEMENTATION, AND MAINTENANCE OF THE LICENSEE'S
6 INFORMATION SECURITY PROGRAM PREPARED BY A DELEGATE AND SHALL
7 RECEIVE A REPORT FROM THE DELEGATE COMPLYING WITH THE REQUIREMENTS
8 OF THE REPORT TO THE BOARD OF DIRECTORS.

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

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

22 (8) AS PART OF ITS INFORMATION SECURITY PROGRAM, EACH LICENSEE
23 SHALL ESTABLISH A WRITTEN INCIDENT RESPONSE PLAN DESIGNED TO
24 PROMPTLY RESPOND TO, AND RECOVER FROM, ANY CYBERSECURITY EVENT THAT
25 COMPROMISES THE CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY OF
26 NONPUBLIC INFORMATION IN ITS POSSESSION, THE LICENSEE'S INFORMATION
27 SYSTEMS, OR THE CONTINUING FUNCTIONALITY OF ANY ASPECT OF THE

1 LICENSEE'S BUSINESS OR OPERATIONS. AN INCIDENT RESPONSE PLAN UNDER
2 THIS SUBSECTION MUST ADDRESS ALL OF THE FOLLOWING AREAS:

3 (A) THE INTERNAL PROCESS FOR RESPONDING TO A CYBERSECURITY
4 EVENT.

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

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

8 (D) EXTERNAL AND INTERNAL COMMUNICATIONS AND INFORMATION
9 SHARING.

10 (E) IDENTIFICATION OF REQUIREMENTS FOR THE REMEDIATION OF ANY
11 IDENTIFIED WEAKNESSES IN INFORMATION SYSTEMS AND ASSOCIATED
12 CONTROLS.

13 (F) DOCUMENTATION AND REPORTING REGARDING CYBERSECURITY EVENTS
14 AND RELATED INCIDENT RESPONSE ACTIVITIES.

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

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

1 THE DIRECTOR.

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

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

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

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

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

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

19 (3) THE LICENSEE SHALL MAINTAIN RECORDS CONCERNING ALL
20 CYBERSECURITY EVENTS FOR AT LEAST 5 YEARS FROM THE DATE OF THE
21 CYBERSECURITY EVENT AND SHALL PRODUCE THOSE RECORDS ON DEMAND OF
22 THE DIRECTOR.

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

1 (A) THIS STATE IS THE LICENSEE'S STATE OF DOMICILE, FOR AN
2 INSURER, OR THIS STATE IS THE LICENSEE'S HOME STATE, FOR AN
3 INSURANCE PRODUCER AS THAT TERM IS DEFINED IN SECTION 1201, AND THE
4 CYBERSECURITY EVENT HAS A REASONABLE LIKELIHOOD OF MATERIALLY
5 HARMING EITHER OF THE FOLLOWING:

6 (i) A CONSUMER RESIDING IN THIS STATE.

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

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

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

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

17 (A) ANY CONSUMER RESIDING IN THIS STATE.

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

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

26 (A) THE DATE OF THE CYBERSECURITY EVENT.

27 (B) A DESCRIPTION OF HOW THE INFORMATION WAS EXPOSED, LOST,

1 STOLEN, OR BREACHED, INCLUDING THE SPECIFIC ROLES AND
2 RESPONSIBILITIES OF THIRD-PARTY SERVICE PROVIDERS, IF ANY.

3 (C) HOW THE CYBERSECURITY EVENT WAS DISCOVERED.

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

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

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

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

16 (H) THE PERIOD DURING WHICH THE INFORMATION SYSTEM WAS
17 COMPROMISED BY THE CYBERSECURITY EVENT.

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

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

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

1 (l) A COPY OF THE LICENSEE'S PRIVACY POLICY AND A STATEMENT
2 OUTLINING THE STEPS THE LICENSEE WILL TAKE TO INVESTIGATE AND
3 NOTIFY CONSUMERS AFFECTED BY THE CYBERSECURITY EVENT.

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

6 (3) A LICENSEE SHALL COMPLY WITH THIS CHAPTER, AS APPLICABLE,
7 AND PROVIDE A COPY OF THE NOTICE SENT TO CONSUMERS UNDER THIS
8 CHAPTER, IF A LICENSEE IS REQUIRED TO NOTIFY THE DIRECTOR UNDER
9 SECTION 559.

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

22 (5) FOR A CYBERSECURITY EVENT INVOLVING NONPUBLIC INFORMATION
23 THAT IS USED BY THE LICENSEE THAT IS ACTING AS AN ASSUMING INSURER
24 OR IN THE POSSESSION, CUSTODY, OR CONTROL OF A LICENSEE THAT IS
25 ACTING AS AN ASSUMING INSURER AND THAT DOES NOT HAVE A DIRECT
26 CONTRACTUAL RELATIONSHIP WITH THE AFFECTED CONSUMERS, THE ASSUMING
27 INSURER SHALL NOTIFY ITS AFFECTED CEDING INSURERS AND THE DIRECTOR

1 OF ITS STATE OF DOMICILE WITHIN 10 BUSINESS DAYS AFTER MAKING THE
2 DETERMINATION THAT A CYBERSECURITY EVENT HAS OCCURRED. THE CEDING
3 INSURERS THAT HAVE A DIRECT CONTRACTUAL RELATIONSHIP WITH AFFECTED
4 CONSUMERS SHALL FULFILL THE CONSUMER NOTIFICATION REQUIREMENTS
5 IMPOSED UNDER THIS SECTION. FOR A CYBERSECURITY EVENT INVOLVING
6 NONPUBLIC INFORMATION THAT IS IN THE POSSESSION, CUSTODY, OR
7 CONTROL OF A THIRD-PARTY SERVICE PROVIDER OF A LICENSEE THAT IS AN
8 ASSUMING INSURER, THE ASSUMING INSURER SHALL NOTIFY ITS AFFECTED
9 CEDING INSURERS AND THE DIRECTOR OF ITS STATE OF DOMICILE WITHIN 10
10 BUSINESS DAYS AFTER RECEIVING NOTICE FROM ITS THIRD-PARTY SERVICE
11 PROVIDER THAT A CYBERSECURITY EVENT HAS OCCURRED. THE CEDING
12 INSURERS THAT HAVE A DIRECT CONTRACTUAL RELATIONSHIP WITH AFFECTED
13 CONSUMERS SHALL FULFILL THE CONSUMER NOTIFICATION REQUIREMENTS
14 IMPOSED UNDER THIS CHAPTER.

15 (6) A LICENSEE ACTING AS AN ASSUMING INSURER DOES NOT HAVE
16 OTHER NOTICE OBLIGATIONS RELATING TO A CYBERSECURITY EVENT OR OTHER
17 DATA BREACH UNDER THIS SECTION OR ANY OTHER LAW OF THIS STATE.

18 (7) FOR A CYBERSECURITY EVENT INVOLVING NONPUBLIC INFORMATION
19 THAT IS IN THE POSSESSION, CUSTODY, OR CONTROL OF A LICENSEE THAT
20 IS AN INSURER OR ITS THIRD-PARTY SERVICE PROVIDER FOR WHICH A
21 CONSUMER ACCESSED THE INSURER'S SERVICES THROUGH AN INDEPENDENT
22 INSURANCE PRODUCER, AND FOR WHICH CONSUMER NOTICE IS REQUIRED UNDER
23 THIS CHAPTER, THE INSURER SHALL NOTIFY THE PRODUCERS OF RECORD OF
24 ALL AFFECTED CONSUMERS OF THE CYBERSECURITY EVENT NOT LATER THAN
25 THE TIME AT WHICH NOTICE IS PROVIDED TO THE AFFECTED CONSUMERS. THE
26 INSURER IS EXCUSED FROM THIS OBLIGATION FOR ANY PRODUCER WHO IS NOT
27 AUTHORIZED BY LAW OR CONTRACT TO SELL, SOLICIT, OR NEGOTIATE ON

1 BEHALF OF THE INSURER, AND IN THOSE INSTANCES IN WHICH THE INSURER
2 DOES NOT HAVE THE CURRENT PRODUCER OF RECORD INFORMATION FOR ANY
3 INDIVIDUAL CONSUMER.

4 SEC. 561. (1) UNLESS THE LICENSEE DETERMINES THAT THE
5 CYBERSECURITY EVENT HAS NOT OR IS NOT LIKELY TO CAUSE SUBSTANTIAL
6 LOSS OR INJURY TO, OR RESULT IN IDENTITY THEFT WITH RESPECT TO, 1
7 OR MORE RESIDENTS OF THIS STATE, A LICENSEE THAT OWNS OR LICENSES
8 DATA THAT ARE INCLUDED IN A DATABASE THAT DISCOVERS A CYBERSECURITY
9 EVENT, OR RECEIVES NOTICE OF A CYBERSECURITY EVENT UNDER SUBSECTION
10 (2), SHALL PROVIDE A NOTICE OF THE CYBERSECURITY EVENT TO EACH
11 RESIDENT OF THIS STATE WHO MEETS 1 OR MORE OF THE FOLLOWING:

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

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

17 (2) UNLESS THE LICENSEE DETERMINES THAT THE CYBERSECURITY
18 EVENT HAS NOT OR IS NOT LIKELY TO CAUSE SUBSTANTIAL LOSS OR INJURY
19 TO, OR RESULT IN IDENTITY THEFT WITH RESPECT TO, 1 OR MORE
20 RESIDENTS OF THIS STATE, A LICENSEE THAT MAINTAINS A DATABASE THAT
21 INCLUDES DATA THAT THE LICENSEE DOES NOT OWN OR LICENSE THAT
22 DISCOVERS A BREACH OF THE SECURITY OF THE DATABASE SHALL PROVIDE A
23 NOTICE TO THE OWNER OR LICENSOR OF THE INFORMATION OF THE
24 CYBERSECURITY EVENT.

25 (3) IN DETERMINING WHETHER A CYBERSECURITY EVENT IS NOT LIKELY
26 TO CAUSE SUBSTANTIAL LOSS OR INJURY TO, OR RESULT IN IDENTITY THEFT
27 WITH RESPECT TO, 1 OR MORE RESIDENTS OF THIS STATE UNDER SUBSECTION

1 (1) OR (2), A LICENSEE SHALL ACT WITH THE CARE AN ORDINARILY
2 PRUDENT PERSON OR AGENCY IN LIKE POSITION WOULD EXERCISE UNDER
3 SIMILAR CIRCUMSTANCES.

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

8 (A) A DELAY IS NECESSARY IN ORDER FOR THE LICENSEE TO TAKE ANY
9 MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE CYBERSECURITY
10 EVENT AND RESTORE THE REASONABLE INTEGRITY OF THE DATABASE.
11 HOWEVER, THE LICENSEE SHALL PROVIDE THE NOTICE REQUIRED UNDER THIS
12 SUBSECTION WITHOUT UNREASONABLE DELAY AFTER THE LICENSEE COMPLETES
13 THE MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE CYBERSECURITY
14 EVENT AND RESTORE THE REASONABLE INTEGRITY OF THE DATABASE.

15 (B) A LAW ENFORCEMENT AGENCY DETERMINES AND ADVISES THE
16 LICENSEE THAT PROVIDING A NOTICE WILL IMPEDE A CRIMINAL OR CIVIL
17 INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY. HOWEVER,
18 THE LICENSEE SHALL PROVIDE THE NOTICE REQUIRED UNDER THIS SECTION
19 WITHOUT UNREASONABLE DELAY AFTER THE LAW ENFORCEMENT AGENCY
20 DETERMINES THAT PROVIDING THE NOTICE WILL NO LONGER IMPEDE THE
21 INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY.

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

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

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

1 (i) THE RECIPIENT HAS EXPRESSLY CONSENTED TO RECEIVE
2 ELECTRONIC NOTICE.

3 (ii) THE LICENSEE HAS AN EXISTING BUSINESS RELATIONSHIP WITH
4 THE RECIPIENT THAT INCLUDES PERIODIC ELECTRONIC MAIL COMMUNICATIONS
5 AND BASED ON THOSE COMMUNICATIONS THE LICENSEE REASONABLY BELIEVES
6 THAT IT HAS THE RECIPIENT'S CURRENT ELECTRONIC MAIL ADDRESS.

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

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

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

14 (ii) THE RECIPIENT HAS EXPRESSLY CONSENTED TO RECEIVE NOTICE
15 BY TELEPHONE, OR IF THE RECIPIENT HAS NOT EXPRESSLY CONSENTED TO
16 RECEIVE NOTICE BY TELEPHONE, THE LICENSEE ALSO PROVIDES NOTICE
17 UNDER SUBDIVISION (A) OR (B) IF THE NOTICE BY TELEPHONE DOES NOT
18 RESULT IN A LIVE CONVERSATION BETWEEN THE INDIVIDUAL REPRESENTING
19 THE LICENSEE AND THE RECIPIENT WITHIN 3 BUSINESS DAYS AFTER THE
20 INITIAL ATTEMPT TO PROVIDE TELEPHONIC NOTICE.

21 (D) SUBSTITUTE NOTICE, IF THE LICENSEE DEMONSTRATES THAT THE
22 COST OF PROVIDING NOTICE UNDER SUBDIVISION (A), (B), OR (C) WILL
23 EXCEED \$250,000.00 OR THAT THE LICENSEE HAS TO PROVIDE NOTICE TO
24 MORE THAN 500,000 RESIDENTS OF THIS STATE. A LICENSEE PROVIDES
25 SUBSTITUTE NOTICE UNDER THIS SUBDIVISION BY DOING ALL OF THE
26 FOLLOWING:

27 (i) IF THE LICENSEE HAS ELECTRONIC MAIL ADDRESSES FOR ANY OF

1 THE RESIDENTS OF THIS STATE WHO ARE ENTITLED TO RECEIVE THE NOTICE,
2 PROVIDING ELECTRONIC NOTICE TO THOSE RESIDENTS.

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

5 (iii) NOTIFYING MAJOR STATEWIDE MEDIA. A NOTIFICATION UNDER
6 THIS SUBPARAGRAPH MUST INCLUDE A TELEPHONE NUMBER OR A WEBSITE
7 ADDRESS THAT A PERSON MAY USE TO OBTAIN ADDITIONAL ASSISTANCE AND
8 INFORMATION.

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

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

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

16 (C) DESCRIBE THE CYBERSECURITY EVENT IN GENERAL TERMS.

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

19 (E) IF APPLICABLE, GENERALLY DESCRIBE WHAT THE LICENSEE
20 PROVIDING THE NOTICE HAS DONE TO PROTECT DATA FROM FURTHER SECURITY
21 BREACHES.

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

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

26 (7) A LICENSEE MAY PROVIDE ANY NOTICE REQUIRED UNDER THIS
27 SECTION UNDER AN AGREEMENT BETWEEN THE LICENSEE AND ANOTHER

1 LICENSEE, IF THE NOTICE PROVIDED UNDER THE AGREEMENT DOES NOT
2 CONFLICT WITH THIS SECTION.

3 (8) EXCEPT AS PROVIDED IN THIS SUBSECTION, AFTER A LICENSEE
4 PROVIDES A NOTICE UNDER THIS SECTION, THE LICENSEE SHALL NOTIFY
5 EACH CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON
6 CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED IN 15 USC 1681A(P), OF
7 THE CYBERSECURITY EVENT WITHOUT UNREASONABLE DELAY. A NOTIFICATION
8 UNDER THIS SUBSECTION MUST INCLUDE THE NUMBER OF NOTICES THAT THE
9 LICENSEE PROVIDED TO RESIDENTS OF THIS STATE AND THE TIMING OF
10 THOSE NOTICES. THIS SUBSECTION DOES NOT APPLY IF EITHER OF THE
11 FOLLOWING IS MET:

12 (A) THE LICENSEE IS REQUIRED UNDER THIS SECTION TO PROVIDE
13 NOTICE OF A CYBERSECURITY EVENT TO 1,000 OR FEWER RESIDENTS OF THIS
14 STATE.

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

16 (9) A LICENSEE THAT IS SUBJECT TO AND COMPLIES WITH THE HEALTH
17 INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, PUBLIC LAW
18 104-191, AND WITH REGULATIONS PROMULGATED UNDER THAT ACT, 45 CFR
19 PARTS 160 AND 164, FOR THE PREVENTION OF UNAUTHORIZED ACCESS TO
20 CUSTOMER INFORMATION AND CUSTOMER NOTICE IS CONSIDERED TO BE IN
21 COMPLIANCE WITH THIS SECTION.

22 (10) A PERSON THAT PROVIDES NOTICE OF A CYBERSECURITY EVENT IN
23 THE MANNER DESCRIBED IN THIS SECTION WHEN A CYBERSECURITY EVENT HAS
24 NOT OCCURRED, WITH THE INTENT TO DEFRAUD, IS GUILTY OF A
25 MISDEMEANOR PUNISHABLE AS FOLLOWS:

26 (A) EXCEPT AS OTHERWISE PROVIDED UNDER SUBDIVISIONS (B) AND
27 (C), BY IMPRISONMENT FOR NOT MORE THAN 93 DAYS OR A FINE OF NOT

1 MORE THAN \$250.00 FOR EACH VIOLATION, OR BOTH.

2 (B) FOR A SECOND VIOLATION, BY IMPRISONMENT FOR NOT MORE THAN
3 93 DAYS OR A FINE OF NOT MORE THAN \$500.00 FOR EACH VIOLATION, OR
4 BOTH.

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

8 (11) SUBJECT TO SUBSECTION (12), A PERSON THAT KNOWINGLY FAILS
9 TO PROVIDE A NOTICE OF A CYBERSECURITY EVENT REQUIRED UNDER THIS
10 SECTION MAY BE ORDERED TO PAY A CIVIL FINE OF NOT MORE THAN \$250.00
11 FOR EACH FAILURE TO PROVIDE NOTICE. THE ATTORNEY GENERAL OR A
12 PROSECUTING ATTORNEY MAY BRING AN ACTION TO RECOVER A CIVIL FINE
13 UNDER THIS SECTION.

14 (12) THE AGGREGATE LIABILITY OF A PERSON FOR CIVIL FINES UNDER
15 SUBSECTION (11) FOR MULTIPLE VIOLATIONS OF SUBSECTION (11) THAT
16 ARISE FROM THE SAME CYBERSECURITY EVENT MUST NOT EXCEED
17 \$750,000.00.

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

20 (14) THIS SECTION APPLIES TO THE DISCOVERY OR NOTIFICATION OF
21 A BREACH OF THE SECURITY OF A DATABASE THAT OCCURS AFTER DECEMBER
22 31, 2019.

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

26 (16) THIS SECTION DEALS WITH SUBJECT MATTER THAT IS OF
27 STATEWIDE CONCERN, AND ANY CHARTER, ORDINANCE, RESOLUTION,

1 REGULATION, RULE, OR OTHER ACTION BY A MUNICIPAL CORPORATION OR
2 OTHER POLITICAL SUBDIVISION OF THIS STATE TO REGULATE, DIRECTLY OR
3 INDIRECTLY, ANY MATTER EXPRESSLY SET FORTH IN THIS SECTION IS
4 PREEMPTED.

5 (17) AS USED IN THIS SECTION:

6 (A) "DATA" MEANS COMPUTERIZED INFORMATION.

7 (B) "IDENTITY THEFT" MEANS A PERSON DOING ANY OF THE
8 FOLLOWING:

9 (i) WITH INTENT TO DEFRAUD OR VIOLATE THE LAW, USING OR
10 ATTEMPTING TO USE THE PERSONAL INFORMATION OF ANOTHER PERSON TO DO
11 EITHER OF THE FOLLOWING:

12 (A) OBTAIN CREDIT, GOODS, SERVICES, MONEY, PROPERTY, A VITAL
13 RECORD, A CONFIDENTIAL TELEPHONE RECORD, MEDICAL RECORDS OR
14 INFORMATION, OR EMPLOYMENT.

15 (B) COMMIT ANOTHER UNLAWFUL ACT.

16 (ii) BY CONCEALING, WITHHOLDING, OR MISREPRESENTING THE
17 PERSON'S IDENTITY, USING OR ATTEMPTING TO USE THE PERSONAL
18 INFORMATION OF ANOTHER PERSON TO DO EITHER OF THE FOLLOWING:

19 (A) OBTAIN CREDIT, GOODS, SERVICES, MONEY, PROPERTY, A VITAL
20 RECORD, A CONFIDENTIAL TELEPHONE RECORD, MEDICAL RECORDS OR
21 INFORMATION, OR EMPLOYMENT.

22 (B) COMMIT ANOTHER UNLAWFUL ACT.

23 (C) "PERSONAL INFORMATION" MEANS THE FIRST NAME OR FIRST
24 INITIAL AND LAST NAME LINKED TO 1 OR MORE OF THE FOLLOWING DATA
25 ELEMENTS OF A RESIDENT OF THIS STATE:

26 (i) A SOCIAL SECURITY NUMBER.

27 (ii) A DRIVER LICENSE NUMBER OR STATE PERSONAL IDENTIFICATION

1 CARD NUMBER.

2 (iii) A DEMAND DEPOSIT OR OTHER FINANCIAL ACCOUNT NUMBER, OR
3 CREDIT CARD OR DEBIT CARD NUMBER, IN COMBINATION WITH ANY REQUIRED
4 SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO
5 ANY OF THE RESIDENT'S FINANCIAL ACCOUNTS.

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.

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 HAS FEWER THAN 25 EMPLOYEES,
17 INCLUDING ANY INDEPENDENT CONTRACTORS, IS EXEMPT FROM SECTION 555.

18 (2) A LICENSEE SUBJECT TO AND IN COMPLIANCE WITH THE HEALTH
19 INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, PUBLIC LAW
20 104-191, AND WITH REGULATIONS PROMULGATED UNDER THAT ACT, IS NOT
21 REQUIRED TO COMPLY WITH THIS CHAPTER EXCEPT FOR THE REQUIREMENTS
22 UNDER SECTIONS 559 AND 561.

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

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

4 (5) THIS CHAPTER TAKES EFFECT ON JANUARY 20, 2021. A LICENSEE
5 SHALL IMPLEMENT SECTION 555 BY JANUARY 20, 2022. HOWEVER, A
6 LICENSEE HAS UNTIL JANUARY 20, 2023 TO IMPLEMENT SECTION 555(6).

7 Enacting section 1. This amendatory act does not take effect
8 unless House Bill No. 6406 of the 99th Legislature is enacted into
9 law.