STATE OF MICHIGAN
DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Bulletin 2021-32-INS

In the matter of:

Insurance Data Security
_____/

Issued and entered
this 10th day of August 2021
by Anita G. Fox
Director

Public Act 690 of 2018 amended the Insurance Code of 1956 (Code) to add Chapter 5A, MCL 500.550 to MCL 500.565, which establishes the exclusive standards for Michigan applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the Director of the Department of Insurance and Financial Services (DIFS). See MCL 500.550.

This bulletin contains a summary description of certain requirements established under Public Act 690 and applicable forms: FIS 2359 (Notice of Cybersecurity Event) and FIS 2360 (Information Security Program Annual Certification). This bulletin should not be relied on as an exhaustive list or comprehensive analysis of the requirements established under Public Act 690. An individual or entity regulated under the insurance laws of Michigan is strongly encouraged to review Public Act 690 to determine the extent to which it applies.

Chapter 5A generally applies to entities that are considered "licensees," defined under MCL 500.553(g) as any of the following:

- An insurer or producer licensed under the Code.
- Any other person licensed or required to be licensed, authorized, or registered under the Code.
- Any other person holding or required to hold a certificate of authority under the Code.

A purchasing group or a risk retention group chartered and licensed in a state other than Michigan or a person acting as an assuming insurer domiciled in a state or jurisdiction other than Michigan is not a licensee for the purposes of Chapter 5A.

Additionally, a licensee subject to and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and federal regulations promulgated under HIPAA is generally not required to comply with Chapter 5A. However, all licensees must comply with MCL 500.559, which requires, in part, notification of cybersecurity events to the Director. MCL 500.565(2).[1]

[1] Pursuant to MCL 500.565(2), without regard to the applicability of and compliance with HIPAA, all licensees must also comply with MCL 500.561, which requires, in part, notification of cybersecurity events to Michigan residences under certain circumstances. However, MCL 500.561(9) states that a licensee subject to and in compliance with HIPAA and federal regulations 45 CFR parts 160 and 164 is considered to be in compliance with MCL 500.561.

Public Act 690 took effect on January 20, 2021. Beginning on that date, licensees must comply with any applicable requirement under Chapter 5A. However, Public Act 690 contains staggered implementation dates that delay certain requirements.

Investigation of Cybersecurity Event
Unexempted licensees are required to conduct a prompt investigation pursuant to MCL 500.557 upon learning that a "cybersecurity event," as defined under MCL 500.553(c), occurred or may have occurred. Licensees are required to maintain records concerning cybersecurity events for at least five years after the event and produce those records upon the Director's demand. MCL 500.557(3).

Notification to DIFS
If criteria listed under MCL 500.559(1)(a) or (b) applies, all licensees are required to notify the Director as promptly as possible, but not later than 10 business days, after a determination that a cybersecurity event occurred involving "nonpublic information," as defined under MCL 500.553(i), in the licensee's possession. Licensees shall utilize FIS 2359 to provide notice to the Director and submit FIS 2359 to DIFS-Cybersecurityforms@Michigan.gov. Pursuant to MCL 500.559(2), licensees shall provide as much information as possible when completing FIS 2359. Licensees have a continuing obligation to update and supplement the information provided to the Director relating to a cybersecurity event and shall also utilize FIS 2359 for that purpose.

Additionally, licensees that are required to provide notification to the Director under MCL 500.559 are required to provide a copy of any notifications provided to a Michigan resident under MCL 500.561, discussed below. See MCL 500.559(3). Licensees shall submit copies of those resident notifications to DIFS-Cybersecurityforms@Michigan.gov. Such copies should be submitted as an attachment to FIS 2359, as directed in that form.

Notification to Michigan Residents
Unexempted licensees that own or license data included in a database are required to provide notification, pursuant to MCL 500.561, of a cybersecurity event without unreasonable delay, as described under MCL 500.561(4), to Michigan residents whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person or whose personal information was accessed and acquired in encrypted form by a licensee with unauthorized access to the encryption key. MCL 500.561(1). A licensee that maintains a database including data it does not own or license is required to provide notice of a cybersecurity event to the owner or licensor of the data, and if the owner or licensor is a licensee under Chapter 5A, that licensee shall comply with the resident-notification requirements under MCL 500.561(1). See MCL 500.561(2).

The notification requirements under MCL 500.561(1) and (2) do not apply if the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft of, one or more Michigan residents. That determination must be made with "the care an ordinarily prudent person or agency in like position would exercise under similar circumstances." MCL 500.561(3).

Licensees should be aware of applicable definitions under MCL 500.553 and MCL 500.561(17), which are not necessarily referenced above. Licensees should also be aware that MCL 500.561 is similar to MCL 445.72 of the Identity Theft Protection Act, which may no longer apply to the licensee due to the exemption provided under MCL 445.64, as added by Public Act 649 of 2018, effective January 20, 2020.

Furthermore, while MCL 500.561 took effect January 20, 2021, MCL 500.561(14) states that it applies to "the discovery or notification of a breach of the security of a database that occurs after December 31, 2019." With respect to security breaches occurring on or after January 1, 2020, and before the effective date of MCL 500.561, DIFS generally considers a licensee in compliance with MCL 500.561 for the purposes of DIFS' regulatory oversight if the licensee provides notifications pursuant to MCL 500.561 without unreasonable delay once MCL 500.561 took effect January 20, 2021, or before that date.

Information Security Program

Not later than January 20, 2022, an unexempted licensee that has 25 or more employees, including any independent contractors, is required to develop, implement, and maintain a "comprehensive written information security program" pursuant to MCL 500.555. If an unexempted licensee does not initially have 25 or more employees and independent contractors, but later reaches or exceeds that threshold, the licensee has 180 days to comply with MCL 500.555. MCL 500.565(4). Additionally, not later than January 20, 2023, unexempted licensees are required to "exercise due diligence in selecting its third-party service provider," as defined under MCL 500.553(l), and require third-party service providers to implement certain measures to protect and secure information systems and nonpublic information in compliance with MCL 500.555(6).

In addition to the exemption for licensees subject to and in compliance with HIPAA and its regulations, a licensee that is an employee, agent, designee, or representative of another licensee is exempt from MCL 500.555 to the extent it is covered by the other licensee's information security program. MCL 500.565(3).

Annual Certification of Information Security Program – Michigan Domiciled Insurers

Not later than February 15 of each year, beginning in 2022, unexempted licensee-insurers domiciled in Michigan must provide the Director a written statement certifying its compliance with MCL 500.555. See MCL 500.555(9). To provide the certification, licensees shall utilize FIS 2360, which will become available on DIFS' website, and submit FIS 2360 to DIFS-Cybersecurityforms@Michigan.gov. Licensees subject to MCL 500.555(9) should be aware that records, data, and schedules supporting the annual certification must be maintained for five years, and the identification of and remedial efforts planned and underway to address areas, systems, or processes requiring material improvement, updating, or redesign must also be documented. This information must be made available for inspection by the Director.

Any questions regarding this bulletin should be directed to:

Department of Insurance and Financial Services
Office of Insurance Evaluation
530 W. Allegan Street, 7th Floor
P.O. Box 30220
Lansing, Michigan 48909-7720
Toll Free: (877) 999-6442

/s/

_____

Anita G. Fox
Director