STATE OF MICHIGAN
GRETCHEN WHITMER
GOVERNOR

MICHIGAN GAMING CONTROL BOARD
DETROIT

HENRY L. WILLIAMS, JR.
EXECUTIVE DIRECTOR

MEMORANDUM

DATE: December 4, 2023

TO: Internet Gaming Operators, Sports Betting Operators, Internet Gaming Platform Providers, Internet Sports Betting Platform Providers (Licensees)

FROM: Dave Murley, Deputy Director

CC: Dave Hicks, Internet Gaming Manager

RE: Protection of PII and Data Breach Notification Requirements

---

LIGA AND LSBA PII PROTECTION AND DATA BREACH NOTIFICATION

Licensees collect and maintain personal identifiable and financial information (PII) while conducting internet gaming and internet sports betting activities pursuant to the Lawful Internet Gaming Act (LIGA) and the Lawful Sports Betting Act (LSBA), respectively. PII is defined in GLI-19 and GLI-33 technical standards adopted by the Board as sensitive information that could potentially be used to identify an individual. Examples of PII include a legal name, date of birth, place of birth, social security number (or equivalent government identification number), driver's license number, passport number, residential address, phone number, email address, debit instrument number, credit card number, bank account number, or other personal information.

Pursuant to Mich Admin Code, R 432.662(h) & 762(h), licensees internal control standards must be designed to ensure wagering account information and PII are adequately protected. As provided by Mich Admin Code, R 432.663(2)(t) & 763(2)(t), the written system of internal controls must include procedures for the security and sharing of PII of an authorized participant, funds or financial information in a wagering account, and other information as required by the Board. The procedures must include how the licensee will provide notice to an authorized participant related to the sharing of PII. Pursuant to Mich Admin Code, R 432.635 & 735, R 432.655(b) & 755(b), and other rules, the licensee must ensure transmitted data and all information in an authorized participant's electronic file is encrypted (or otherwise securely transmitted or stored) to ensure the integrity and confidentiality of such data. In addition, licensees must comply with GLI-19 and GLI-33 technical standards, adopted by the Board, which contain several requirements designed to ensure that wagering account and PII are adequately protected and include related privacy policy requirements.

In the event a data breach does occur, licensees, in accordance with their internal controls, must immediately notify the Board. See Mich Admin Code, R 432.628b & 728b, and Board's Notice of Requirement memo, dated May 4, 2022.

OTHER LEGAL AND REGULATORY REQUIREMENTS

All licensees must be knowledgeable of and comply with all relevant state and federal law regarding the protection of PII and handling of data breaches. These requirements include, but are not limited to, the following:

Gramm Leach Bliley Act

The Gramm Leach Bliley Act (GLBA) imposes an affirmative and continuing obligation on financial institutions to protect the security and confidentiality of customers' nonpublic personal information. Financial institutions are institutions which conduct financial transactions, including exchanging, transferring, and safeguarding money. 15 USC 6801(a).

The GLBA requires financial institutions to develop, implement, and maintain a comprehensive security program reasonably designed to protect against the unauthorized use of customer information that could result in substantial harm or inconvenience. See 15 USC 6801(b)(3) & 16 CFR 314.3(a) & 314.3(b)(3).

The GLBA prescribes additional requirements in the event of a data breach which include, but are not limited to, notifying the relevant federal regulator of the incident, notifying customers in some instances, and filing a Suspicious Activity Report as required by the Bank Secrecy Act.

Bank Secrecy Act

The Bank Secrecy Act (BSA) may be relevant in cases of a data breach. The BSA requires certain financial institutions to file reports on possible criminal activity. 31 USC 5311(1)(A). The BSA applies to commercial and tribal casinos with an annual gaming revenue of more than $1,000,000.00. 31 USC 5312(a)(2)(X). In certain cases, a Suspicious Activity Report must be filed with Financial Crimes Enforcement Network, which will trigger reporting pursuant to GLBA, LIGA, and LSBA.

Michigan Identity Theft Protection Act

The purpose of the Identify Theft Protection Act (ITPA) is to require notification of a security breach of a database containing personal information. Specifically, businesses must notify Michigan residents when an unauthorized individual has accessed or acquired personal information from the business' database unless the security breach "has not or is not likely to cause substantial loss or injury or result in identity theft[.]" MCL 445.72(1).

The ITPA requires businesses to provide this notice "without unreasonable delay." MCL 445.72(4). A delay may be reasonable to determine the scope of the security breach and restore

the integrity of the database, or when a law enforcement agency advises that sending out the notice would impede a criminal or civil investigation or compromise homeland or national security.

NOTIFICATION REQUIREMENTS

In accordance with the LIGA, the LSBA, and their respective rules, licensees must adhere to internal controls approved procedures and do the following in the event of a data breach:

1. Immediately notify the Board in the event of any data breach. The notification must include all information prescribed in the Board's Notice of Requirement memo, dated May 4, 2022, which is enclosed for your convenience. The notification must be clearly marked "data breach" to ensure the Board can identify the nature of the notifications. The notification must be sent to MGCB-Igaming@michigan.gov. The notification must include all of the following in addition to the information required in the Board's May 4, 2022, Notification Requirements memo as well as the following:

    - A description of the extent of the data breach which includes, but is not limited to, information on number of individuals whose PII was compromised and the type of PII compromised because of the data breach. Describe and quantify the direct and indirect impact the data breach had on those impacted such as financial loss, inconvenience, etc.

    - A description of all notifications that have been sent or must be sent to impacted individuals and the information that was shared with such individuals. The Board expects that the notification will at a minimum provide information on the licensees responsibility for protecting PII, inform all impact individual of the steps the licensee is performing to protect their PII, explain the resources that are available to the impacted individual such as free identify theft projection/credit monitoring services), and indicate whether the licensee intends to reimburse the impacted individual in the event of actual loss caused by the data breach.

2. Review and update internal controls, as necessary, to ensure PII is protected, data breaches are properly addressed, and that all required notifications (including those to customers) are properly remitted.

3. Review and update internal controls, as necessary, to ensure any third parties in which you share PII with have adequate controls in place to protect such data. Licensees are responsible for compliance regardless of whether any third party was responsible or partly responsible for the data breach.

The Board anticipates that some notification information may not be available to the licensee at the time a data breach occurs or is discovered. In those circumstances, a licensee may submit a preliminary notification immediately and follow-up with a final detailed notification which includes all required information shortly thereafter. Failure to protect PII and/or notify the Board in the event of a data breach may result in disciplinary action.