STATE OF MICHIGAN
GRETCHEN WHITMER
GOVERNOR

MICHIGAN GAMING CONTROL BOARD
DETROIT

HENRY L. WILLIAMS JR.
EXECUTIVE DIRECTOR

TECHNICAL BULLETIN No. 2024-03
GEOFENCING SPECIFICATIONS
Revised February 28, 2024

This technical bulletin applies to internet gaming conducted pursuant to the Lawful Internet Gaming Act (LIGA), 2019 PA 152, and internet sports betting conducted pursuant to the Lawful Sports Betting Act (LSBA), 2019 PA 149. Without limitation, the following are subject to this technical bulletin:

(1) Internet gaming operators and sports betting operators (operator or operators).
(2) Internet gaming platform providers and internet sports betting platform providers (platform provider or platform providers).
(3) Internet gaming platforms and internet sports betting platforms (platform or platforms).
(4) Internet gaming suppliers and sports betting suppliers (supplier or suppliers).
(5) Vendors registered under the LIGA and/or the LSBA (vendor or vendors).
(6) Internet wagers and internet sports betting wagers (wager or wagers).
(7) Internet wagering accounts and internet sports betting accounts (account or accounts).

Under R432.631(1), the LIGA, as amended, and R432.731(1) all internet gaming/internet sports betting transactions conducted pursuant to the LIGA and LSBA must be initiated and received or otherwise made by an authorized participant located in the state of Michigan or, if the Michigan Gaming Control Board (Board) authorizes multijurisdictional internet sports betting in accordance with the LSBA or internet poker in accordance with LIGA, another jurisdiction in the United States authorized by the multijurisdictional agreement.

Under R432.631(2) and R432.731(2), an operator and its platform provider must utilize a geofencing system to reasonably detect the physical location of an individual or authorized participant attempting to access the platform and place a wager and to monitor and block unauthorized attempts to access the platform and place a wager when the individual or authorized participant is not within the permitted boundary.

Under R432.631(3) and R432.731(3), the geofencing system must ensure that any individual or authorized participant is located within the permitted boundary when placing any wager and must be equipped to dynamically monitor the individual's or authorized participant's location and block unauthorized attempts to access the platform in order to place a wager throughout the duration of the authorized participant session.

Under R432.631(4) and R432.731(4), the Board shall approve all technical specifications for geofencing and any specific requirements related to geofencing technology that is commercially available. Accordingly, the Board prescribes the following geofencing technical specifications and requirements:

(1) Applicable Definitions

(a) "Geofence" means, for the purpose of this technical bulletin, a virtual geographic perimeter defined by a Global Positioning System (GPS), Radio-frequency Identification (RFID), or other similar technology, which enables software to trigger a response when an individual's or authorized participant's device enters or leaves a predefined set of boundaries.

(b) "Geofencing System" means, for the purpose of this technical bulletin, a process to reasonably detect the geolocation of an individual or authorized participant when said individual or authorized participant is attempting to access the platform and place a wager.

(c) "Permitted boundary" means, for the purpose of this technical bulletin, the geographic boundaries of the state of Michigan, including Indian land located in the state of Michigan to the extent allowed by applicable state and federal law. If the Board authorizes multijurisdictional internet sports betting in accordance with the LSBA or internet poker in accordance with LIGA, the permitted boundary includes the geographic boundaries of any other jurisdiction in the United States authorized by a multijurisdictional agreement, subject to any limitations provided in the multijurisdictional agreement, any applicable state or federal law, or as otherwise prescribed by the Board.

(2) Technical Specifications

Frequency of the System
To ensure an individual or authorized participant is located within the permitted boundary, the Geofencing System must be fully equipped to dynamically monitor the individual's or authorized participant's location and block unauthorized attempts to access the platform in order to place a wager throughout the duration of the authorized participant session.

The platform must trigger:

(a) A geolocation check prior to the placement of the first wager in the authorized participant session.

(b) Recurring periodic geolocation checks. If an authorized participant session is longer than a single wager, the recurring periodic geolocation check must be administered as follows:
   (i) Static connection: Recheck every twenty (20) minutes, or five (5) minutes if within one (1) mile of the border of the permitted boundary.
   (ii) Mobile connections: Recheck intervals to be based on an individual's or authorized participant's proximity to the border of the permitted boundary, with an assumed travel velocity of seventy (70) miles per hour and a maximum interval not exceeding twenty (20) minutes.

(c) The operator and platform provider must define the reasons for all trigger instances (e.g., single wager, deposit, etc.) and communicate the trigger reason using an anonymized user ID (i.e., no names or personal data collected) to the Geofencing System when requesting each geolocation check.

(d) A geolocation check must be conducted immediately upon the detection of a change of the individual's or authorized participant's internet protocol (IP) address.

(e) If the platform determines that an individual or authorized participant is located outside the permitted boundary, the individual or authorized participant must be provided limited access to the platform and to their account. The individual or authorized participant must also be prohibited from placing a wager until a geolocation re-check is performed and confirms the individual or authorized participant is located within the permitted boundary.

Location Data Accuracy
To ensure location data is accurate and reliable, the Geofencing System must:

(a) Utilize pinpointed and accurate location data sources to confirm the individual or authorized participant is located within the permitted boundary.
    (i) When a mobile carrier's data is used, the individual's or authorized participant's device (where the authorized participant session occurs) and the mobile carrier's data source (i.e., mobile device) must be in proximity to each other.

(b) Disregard IP location data for devices utilizing mobile internet (e.g., 3G, 4G, 5G, LTE) connections.

(c) Possess the ability to control whether the accuracy radius of the location data source is permitted to overlap or exceed defined buffer zones or the permitted boundary.

To mitigate and account for discrepancies between mapping sources and variances in geospatial data, and to ensure accuracy of locational data, the Geofencing System must:

(a) Utilize boundary polygons based on audited maps.

(b) Overlay location information onto these boundary polygons.

The geolocation method shall monitor and flag for investigation any wagers placed by a single account from geographically inconsistent locations during a single authorized participant session.

Location Data Integrity
To ensure the integrity of an individual's or authorized participant's location data, the Geofencing System must:

(a) Detect and block any locational data fraud, including but not limited to proxy servers, fake location applications, virtual machines, remote desktop programs, etc.

(b) Utilize detection and blocking mechanisms verifiable to a source code level.

(c) Follow best practice security measures to stop "man in the middle" attacks and prevent code manipulation such as replay attacks.

Device Integrity
To ensure the integrity of any device used by an individual or authorized participant, the Geofencing System must detect and block non-secure devices and those which indicate any system-level tampering (e.g., rooting, jailbreaking, etc.).

Authorized Participant Integrity
To ensure the integrity of an individual or authorized participant, the Geofencing System must detect and flag for investigation any individuals or authorized participants who make repeated unauthorized attempts to access the platform.

Reporting and Analytics
All location fraud must be assessed on a single geolocation check, as well as on a cumulative basis of an individual's or authorized participant's history over time. The Geofencing System must provide the Board, and operators and/or platform providers with a real-time dashboard and data feed which:

(a) Is customizable and displays geolocation data and visuals on demand.

(b) Displays and is filterable by, at a minimum, the following data:
   i. Time period.
   ii. Username.
   iii. Operator and/or platform provider name.
   iv. Device identifier.
   v. City, state and country.
   vi. Passed or failed transactions and failure reasons.
   vii. IP address.
   viii. Device type and operating system.

(c) Provides an interactive mapping tool capable of:
   i. Displaying locations of geolocation transactions.
   ii. Geofencing to identify each building location.
   iii. Using coordinates to pinpoint locations.

(d) Provides data, visuals and reporting of suspicious activity including:
   i. Malicious or repeated location spoofing.
   ii. Account sharing and device sharing.
   iii. Other high-risk transactional data.

System Maintenance
To verify the overall integrity of the Geofencing System, it must:

(a) Be reviewed regularly to assess and measure its continued ability to detect and mitigate existing and emerging location fraud risks.

(b) Undergo frequent updates, at least one every three months, to maintain cutting-edge data collection, device compatibility, and fraud prevention capabilities.

(c) Utilize databases (IP, proxy, fraud, etc.) that are updated daily, at a minimum, and are not open source.

(3) Geolocation Error Messages to Individuals and Authorized Participants

The operator and its platform provider must implement a delivery mechanism to send a message to an individual or authorized participant to notify the user of a geolocation failure which address all, but are not limited to, the following scenarios:

(a) A geolocation result exceeds a Board approved threshold, or insufficient geolocation is obtained for the individual or authorized participant.

(b) The geofencing system detected potential location fraud.

(c) Software is found running on the individual's or authorized participant's device which could be used to circumvent geolocation.

(d) Not enough location data or data accuracy is low.

(e) The IP address is located outside the permitted boundary.

(f) The device is too close to border of another state or country.

(g) The device is running an IP anonymizer.

(h) A proxy was detected.

(i) The device does not have latest required version of geolocation software installed.

(j) Location jumping/account sharing and advanced fraud risk.

(k) Remote desktop software was detected.

(l) Mobile device tampering was detected.

Notwithstanding the minimum standards established in this technical bulletin, operators and its platform provider must employ reasonable efforts to ensure it meets or exceeds current industry-recognized geofencing standards. The Board reserves the right to reassess or clarify the standards established in this technical bulletin at any time in response to a legal interpretation, to include additional standards the Board deems appropriate, to adjust to changes in technology, relevant standards, or platform design, or for any other reason necessary to regulate internet gaming under the LIGA or internet sports betting under the LSBA.