CHAPTER 809b. GEOLOCATION – TECHNICAL STANDARDS

§ 809b.7. Geolocation.

(a) The following words and terms, when used in this section, have the following meanings, unless the context clearly indicates otherwise:

Geo-fence – A virtual geographic boundary that enables software to trigger a response when an internet connected device or mobile device enters or is situated in a particular area.

Jailbreaking – Modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator to allow the installation of unauthorized software.

Man-in-the-Middle Attack – An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Rooting – Attaining root access to the Android operating system code to modify the software code on the device or install software that the manufacturer would not allow to be installed.

(b) An interactive gaming system shall have a geolocation system that detects the physical location of a player at the following times, at a minimum:

(1) When a player first logs into the interactive gaming system or makes an initial bet or wager using the interactive gaming system.

(2) If an interactive gaming session is longer than a single bet or wager and the player is using a static connection or mobile internet connection, a geolocation re-check shall be performed every 20 minutes, or 5 minutes if the player is located within 1 mile of the border of the Commonwealth.

(3) If an interactive gaming session is longer than a single bet or wager and the player is using a mobile internet connection, a geolocation re-check shall be performed within a reasonable time interval based upon a player’s proximity to the boundary line of an excluded zone with an assumed travel velocity of 65 miles-per-hour.

(4) If an interactive gaming system is designed to perform a geolocation check when a player first logs into the interactive gaming system and it is determined that the player is located outside of the Commonwealth or within one of the Geo-fence boundary areas described in subsection (e) of this Chapter, the player must be provided limited access to the interactive gaming account functions of the interactive gaming system, but must be prohibited from placing a bet or wager until a geolocation re-check is performed that confirms the player is within the Commonwealth and/or is no longer within a Geo-fence boundary area.

(c) To ensure that the collected location data is accurate and reliable, the geolocation system shall:

(1) Utilize pinpoint accurate location data sources to confirm the player is located within the permitted boundary.

(i) When the gaming session is initiated by a mobile internet connection, the player's device where the gaming session occurs and the mobile internet source must be in proximity to each other.

(2) Disregard Internet Protocol, or IP location data for devices utilizing mobile internet connections.

(3) Discount IP location data for all other connections such that it shall not be used as the primary location data source.

(4) Possess the ability to control that the location data accuracy radius cannot be within boundary buffer zones or over the boundary line.

(d) To account for discrepancies between mapping sources and variances and geolocation data and to ensure accuracy of location data, the geolocation system shall:

(1) Utilize boundary polygons based upon modified Commonwealth defined and audited maps.

(2) Overlay collected location data onto these boundary polygons.

(e) To ensure compliance with 4 Pa.C.S. § 13B63(c) (relating to Internet Cafes and prohibition), the geolocation system shall have Geo-fence capability, which shall:

(1) Establish a defined Geo-fence boundary generally around the interior walled-perimeter that surrounds the Gaming Floor of all Licensed Facilities within the Commonwealth.

(2) Detect and block a registered player from placing a wager while within one of the above-described Geo-fence boundaries.

(f) To ensure integrity of location data, the geolocation system shall:

(1) Detect and block location data fraud, including but not limited to Proxy, Fake Location Apps, Virtual Machines, and Remote Desktop Programs.

(2) Utilize detection and blocking mechanism verifiable to a source code level.

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

(g) To ensure integrity of a player's device, the geolocation system shall detect and block non-secure devices and/or those which indicate system-level tampering (i.e. rooting, jailbreaking).

(h) To ensure integrity of a player, the geolocation system shall detect and block players that make repeated unauthorized attempts to access the interactive gaming system or place wagers while not in a permitted location.

(i) To ensure integrity of the geolocation checks and to prevent fraud, the geolocation system shall:

(1) Use a non-open-source location data database that is updated daily.

(2) Display a real-time data feed of all geolocation checks and re-checks and potential fraud risks.

(3) Possess alert systems to identify unauthorized or improper access to the interactive gaming system.

(4) Provide routine, recurrent delivery of supplemental fraud reports pertaining to suspicious activities, account sharing, malicious players and devices, as well as other high risk transactional data, with such reports to be shared with the interactive gaming certificate holder or interactive gaming operator.

(j) To ensure and verify integrity of the geolocation system, the geolocation system shall:

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

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

(k) To ensure future protection and integrity of the geolocation system, the interactive gaming certificate holder or interactive gaming operator shall monitor technology trends and advancements in geolocation fraud, and shall continually monitor and update the geolocation system to reasonably protect against geolocation fraud based upon these trends and advancements.