MERCADIEN, P.C.
CERTIFIED PUBLIC ACCOUNTANTS

December 11, 2023

Audit Committee and Management
of the State of New Jersey
Division of State Lottery
One Brunswick Circle
P.O. Box 041
Trenton, NJ 08625-0041

[redacted] INC. CYBERSECURITY TECHNIQUES AND TECHNOLOGY

This letter includes observations with respect to matters that came to our attention in connection with our monthly audit procedures of [redacted] Inc. ("[redacted] lottery courier service ("service agreement") for the month ended June 30, 2023, pertaining to the cybersecurity techniques and technology standards it utilized. The observations are provided to establish compliance with the cybersecurity techniques and technology standards for New Jersey couriers under the Courier Services Act, P.L. 2017, c. 11 and the State of New Jersey State Lottery (the "Lottery") regulations, Subchapter 12, Courier Services (hereinafter collectively referred to as the "Courier Services Laws").

**Audit Objective**

The monthly audit objective was to determine if the cybersecurity policies and procedures adopted, implemented and operated by [redacted] aligned with the Courier Services Laws and met cybersecurity best practices as guided by the National Institute of Standards and Technology ("NIST") Cybersecurity Framework and the Center for Internet Security ("CIS").

**Scope**

The scope of our monthly cybersecurity procedures was limited to certain operations and associated transactions of [redacted] occurring under the service agreement with the Lottery for the month ended June 30, 2023.

**Methodology**

To accomplish our objective, we inquired of [redacted] management and reviewed documentation provided by [redacted] pertaining to its cybersecurity policies and procedures, IT system audit logs, internal compliance reports, and third-party security audit reports and compared the material and the adoption of their policies and techniques against industry standards such as the NIST Cybersecurity Framework and general industry best practices.

**Cybersecurity Program (A)**[i]

Risk: Exposure, loss, exploitation of company and customer data by unauthorized individuals (internally and externally).

Control: Written Information Security Policies and Procedures.

Testing of Control:

We were informed there were no updates to [redacted] written Infosec Policies and Procedures during this period.

**Identity Checks/Payment Validation (E, F)** [1]

Risk: Courier sales of lottery tickets to customers not of legal age.

Control: Utilizes the services of a third-party provider (IDology, a GBG Company) to screen its customers at the time they create and fund their accounts.

Testing of Control:

We obtained and reviewed the following data sets provided by [redacted] from its database system for June 2023: Age verification (titled E.a. Vendor Exception verification fail report and addresses for 100 random new accounts (titled E.c. - 100 Random Accounts).

The Vendor Exception report shows 494 players failed the registration process by reason of age, address or phone number.

The report of 100 random new accounts titled "E.c. - 100 Random Accounts" did not include anyone who was under 18 as of the date their account was opened.

Our review of the controls used by [redacted] to prevent underage customers from purchasing lottery tickets confirmed they operated consistently with their intended results without exceptions for June 2023.

**GPS Technology (D)** [1]

Risk: Customers purchasing tickets who are not physically within the geographic boundaries of the State of New Jersey at the time an order is placed.

Control: Use of a third-party service provider (Geocod.io) to confirm the location of a customer when they: (i) open the application, (ii) attempt to add funds, and (iii) place an order for a drawing.

Testing of Control:

Successful gameplay GPS logs for the month of June 2023 were provided. Upon analysis of the GPS coordinates for successful play, no geographical anomalies were noted.

**Data Storage/Backup/Email Security (J, M)** [1]

Risk:

1. Software applications and customer data are operating and stored outside of the United States beyond the jurisdictional reach of the Lottery.

2. Customer data is lost or becomes unavailable due to technical errors, unauthorized access, or loss of integrity.

3. Company and customer electronic communications become compromised and business and personally identifiable information exposed to third parties.

Controls:

1. Use of servers based in the United States.

2. Use of cloud-based data backup vendor.

3. Cybersecurity training for employees, two-factor authentication for company email accounts, and domain security features.

Testing of Controls:

We requested evidence of [redacted] database backups. We requested confirmation that employee cybersecurity training is occurring, employee test scores, and written confirmation of receipt by employees of a cybersecurity training manual.

We requested evidence showing two-factor authentication was in use for [redacted] back-office system and its email accounts and the status of [redacted] email domain security.

Observations:

[redacted] produced a spreadsheet exported from its system (snapshots-20230601T100424.csv and policies-20230601T100417.csv) listing the dates the backups for its checkout-production and accounting-production databases were created for June 2023 as well as evidence of backup retention. [redacted] procedures for backing up its data meet the Lottery's regulatory requirements for location and length of storage and meet generally acceptable cybersecurity standards.

[redacted] provided a screenshot of its Google Console (Google Workspace MFA Settings - June 2023.png) as well as various screenshots of the login and authentication process dated June 1, 2023, to confirm two-factor authentication is enforced for access to its Google Cloud environment, including email. [redacted] procedures for securing its data meet generally acceptable cybersecurity standards.

Regarding email domain security, [redacted] provided evidence in the form of screenshots that they have implemented DMARC, DKIM and SPF – technology that authenticates email senders by verifying where the email originated.

With respect to [redacted] security awareness training program, [redacted] produced a chart of its employee training schedule for June titled "Cybersecurity Training Audit as of 07.03.23" which shows its employee training program began on February 7, 2023, on a variety of topics. Of the five employees who had been registered by the company in June to take the training, all but one had completed their assignments by the end of the month. As previously reported, employees can request they be provided with additional time to complete the training.

**Password Management/Securing PII (G, H, I, M)** [1]

Risk: Exposure of company and customer data to unauthorized third parties.

Controls: Use of one-time passwords, white-listing of IP addresses to access databases, and segregation of credentials.

Testing of Controls:

We requested a log of one-time passwords issued to users, a log of administrative password changes for June 2023, a log of white-listed IP addresses authorized to access databases containing customer data, a log of successful logins to the databases, and a log of failed login attempts to those databases. We also requested evidence that all available software patches on all systems have been addressed/remediated for any critical or high-level patches.

Observations:

We reviewed the following logs provided by [redacted] password_changes.csv, failed_logins.csv, and successful_logins.csv, as well as a list of white-listed IP addresses. This information indicates [redacted] continues to utilize controls to limit administrative access to only authorized accounts.

We reviewed a chart of software updates (M.b. - List of software updates) which shows updates and the status of its application environment during the month of June 2023. The chart confirms its change process aligns with their Information Security Policy.

The macOS Version Log - June 2023.csv and Webroot User Report - June 2023 shows that workstations (Mac and PC) used by [redacted] employees have antivirus tools installed and maintained, per policy.

**Breach Detection and Incident Response (M, N)** [1]

Risk: Delayed response to a suspected or actual data breach can lead to prolonged exposure of company and customer data to unauthorized third parties.

Controls: Written policy and procedures for responding to a data breach, use of internal communication tools to alert employees of a suspected/actual breach, use of antivirus software and a managed cloud security third-party service.

Testing of Controls:

We requested all cybersecurity Incident Reports created by employees. We requested logs of cybersecurity monitoring service alerts and corresponding responses.

Observations:

Collateral provided included screenshots dated July 2, 2023, of its Cloudflare dashboard Analytics relating to cybersecurity incidents for June 2023. [redacted] confirmed it acts on notifications that are irregular, unusual, or massive and attested that "…no threats above a 'low' status or fit criteria for review…" were received, which corresponds to the screenshots provided.

As previously discussed, [redacted] implemented Webroot for antivirus protection of its endpoints. While Webroot's principal means of detecting malicious activity is passive, combined with other threat detection tools and activities utilized by [redacted] it meets the cybersecurity techniques and technology standards for New Jersey couriers at this time.

Management advised it is continuously assessing its cyber risk exposure and is currently evaluating additional controls to reduce its "threat surface."

**Third-Party Cybersecurity Testing Assurances (K, M, N)** [1]

Risk: Courier service system not operating as designed to protect against unauthorized access to company and customer data.

Draft
Control: Independent testing labs used to verify/validate technology is operating as expected.

Testing of Control:

We requested copies of penetration test reports, vulnerability scans and cybersecurity monitoring reports for June 2023. Management confirmed no testing occurred during this period.

This letter is intended solely for the information and use of the audit committee, management and others within the Lottery, and is not intended to be and should not be used by anyone other than these specified parties. We appreciate serving the Lottery and would be happy to assist you in addressing any of the suggestions in this letter.

*Mercadien, P.C.*
*Certified Public Accountants*

[i] As used herein, letter references relate to the required audit categories set forth in the NJ Division of State Lottery Commission's Bid #19DPP00377 section 3.1.5.