

# IN THE MISSOURI GAMING COMMISSION

In Re: )  
 ) DC-13-702  
Penn National Gaming, Inc. )

## PRELIMINARY ORDER FOR DISCIPLINARY ACTION

Comes now the Missouri Gaming Commission acting in its official capacity pursuant to 11 CSR 45-13.050, and states as follows:

1. The Missouri Gaming Commission (the "Commission") or ("MGC") is a state commission created under Chapter 313, RSMo 2000, with jurisdiction over gaming activities, including riverboat gambling activities, in the State of Missouri.
2. The Commission issued Penn National Gaming, Inc. (the "Company"), a Class A gaming license to develop and operate Class B gaming licenses in the State of Missouri.
3. Penn National Gaming, Inc. is the parent organization or controlling entity of St. Louis Gaming Ventures, LLC d/b/a Hollywood Casino St. Louis.
4. The Commission issued a Class B riverboat gambling license to Missouri Gaming Company ("Company"), to conduct games on and operate the excursion gambling boat known as St. Louis Gaming Ventures, LLC d/b/a Hollywood Casino St. Louis ("Casino").
5. As the holder of a Class A license, the Company is subject to the provisions of Sections 313.800 to 313.850, RSMo. 2000, and the regulations promulgated thereunder by the Commission.

### STATEMENT OF FACTS<sup>1</sup>

6. On January 28, 2013, Electronic Gaming Device (EGD) Specialist Drew Biermann contacted Hollywood Casino St. Louis (HCSTL) Market Engineer Jeff Reichert about missing November remote logs.
7. After speaking with Reichert and Regulatory Compliance Manager Jeff Hendricks, Beirman learned:

---

<sup>1</sup> 20130227004

- a. On January 28, 2013, it was discovered that Aristocrat Technologies, Inc. (“ATI”) had remote access into the Hollywood St. Louis slot accounting system via a temporary Penn National corporate IT account. This account was established by Penn National Corporate IT before the Harrah’s /Hollywood St. Louis acquisition occurred and was not disabled following the opening of Hollywood St. Louis.
- b. The remote access, via the corporate IT account, permitted ATI to remote into the Hollywood St. Louis slot accounting system without the local IT department having to authenticate the session.
- c. By ATI using the Penn National corporate IT account, the Hollywood St. Louis local IT department was unaware of the remote access and did not submit the required monthly remote access logs to the MGC.

### LAW

8. Under Section 313.805(6), RSMo 2000, the Commission may assess any appropriate administrative penalty against a licensee, including but not limited to, suspension, revocation or penalties of an amount determined by the Commission.
9. Under Section 313.812.14, RSMo 2000, a holder of any license is subject to imposition of penalties, suspension or revocation of such license for any act or failure to act by himself or his agents or employees, that is injurious to the public health, safety, morals, good order and general welfare of the people of the state of Missouri, or that would discredit or tend to discredit the Missouri gaming industry or the state of Missouri.
10. Under Section 313.812.14(1), RSMo 2000, a licensee may be disciplined for failing to comply with or make provisions for compliance with Sections 313.800 to 313.850, the rules and regulations of the commission or any federal, state or local law or regulation.
11. Under Section 313.812.14(2), RSMo 2000, a licensee may be disciplined for failing to comply with any rule, order or ruling of the Commission or its agents pertaining to gaming.
12. Under 11 CSR 45-9.060(3), violations of the minimum internal control standards (“MICS”) by a Class A licensee or an agent or employee of a Class A licensee are deemed to be unsuitable conduct for which the Class A licensee and/or its agent or employee is subject to administrative penalty pursuant to section 313.805(6), RSMo and 11 CSR 45-1 et seq., as amended from time to time. Any agent or employee of a Class A licensee that is involved in a violation of the minimum internal control standards may be subject to fine, discipline or license revocation.
13. Under 11 CSR 45-9.060(4), violations of the Class A licensee’s internal control system (“ICS”) by the Class A licensee or an agent or employee of the Class A

licensee shall be prima facie evidence of unsuitable conduct for which the Class A licensee and/or its agents or employees may be subject to discipline pursuant to Section 313.806(6), RSMo, and 11 CSR 45-1 et seq., as amended from time to time.

14. The Missouri Internal Control Standards (MICS) Chapter S, § 12.01 states, All remote access connections to the Critical IT System(s) shall be granted/authorized through the use of Two-Factor Authentication (T-FA).

15. The Missouri Internal Control Standards (MICS) Chapter S, § 12.04 states, Vendor remote access shall require:

- (A) Each remote access to a Critical IT System application shall only be granted by a Class A or Class B licensed MIS employee and shall be documented on the Remote Access Log which shall be submitted to the MGC EGD Department by the 10th day of each month;
- (B) Whenever the remote access connection is not in use it shall be physically or logically disabled to prevent access. Remote access shall be enabled only when approved by a Class A or Class B licensed MIS employee;
- (C) User accounts required to establish remote access to remain disabled on all operating systems, databases, network devices, and applications until needed. Subsequent to an authorized use by a vendor, the account shall be returned to a disabled state immediately; and
- (D) The Critical IT System or the operating system to automatically monitor and record the user account name, time and date the connection was made, duration of the connection, and activity while connected, including the specific areas accessed and changes made.

16. The Company's Internal Control Standards (ICS) Chapter S, § 12.01 states, All remote access connections to the Critical IT System(s) shall be granted/authorized through the use of Two-Factor Authentication (T-FA).

17. The Company's Internal Control Standards (ICS) Chapter S, § 12.03 states, Hollywood Casino St. Louis' remote access to Critical IT systems will be established in the following manner:

- 1. The Requestor must submit a request to IT via the IT electronic issue tracking system.
- 2. The Director of Information Technology and appropriate department Executive must approve of the request.
- 3. The Director of Information Technology, Market Engineer, Support Specialist Desktop and IT Systems Administrator will enable remote access.
- 4. Remote access is established via the user's Active Directory account which includes the following security features:
  - a. Password expires every 90 days
  - b. Minimum of 6 characters
  - c. Complex password features

- d. Account is locked after 3 unsuccessful login attempts and can only be unlocked by IT personnel
- 5. Remote access is facilitated via secure web-based VPN portal.

18. The Company's Internal Control Standards (ICS) Chapter S, § 12.04 states, Vendor remote access shall require:

- (A) Each remote access to a Critical IT System application shall only be granted by a Penn National Gaming, Inc. or Hollywood Casino St. Louis licensed MIS employee and shall be documented on the Remote Access Log which shall be submitted to the MGC EGD Department by the 10th day of each month;
- (B) Whenever the remote access connection is not in use it shall be logically disabled to prevent access by disabling the remote access account. Remote access shall be enabled only when approved by a Penn National Gaming, Inc. or Hollywood Casino St. Louis licensed MIS employee;
- (C) User accounts required to establish remote access to remain disabled on all operating systems, databases, network devices, and applications until needed. Subsequent to an authorized use by a vendor, the account shall be returned to a disabled state immediately; and
- (D) The Critical IT System or the operating system to automatically monitor and record the user account name, time and date the connection was made, duration of the connection, and activity while connected, including the specific areas accessed and changes made. 12.04(D) is accomplished by channeling all remote access from ATI through a single dedicated server. This server is equipped with TSMonitor monitoring software that records all activity during the remote access session.

### **VIOLATIONS**

19. The actions or omissions of employees or agents of the Company as described above constitute a failure to properly secure their critical IT systems. The conduct as alleged is a violation of The Commission's MICS Chapter S, § 12.01, 12.03 and 12.04; The Company's ICS, Chapter S, § 12.01, 12.03 and 12.04. Company is subject to discipline for such violations under 11 CSR 45-9.063(3) & (4), AND sections 313.805(6), 313.812.14 and 313.812.14(1) & (2) RSMo.

### **PENALTY PROPOSED**

20. Under Section 313.805(6), RSMo 2000, the Commission has the power to assess any appropriate administrative penalty against the Company, as the holder of a Class A license.

21. THEREFORE, it is proposed that the Commission fine Penn National Gaming, Inc. the amount of \$5,000 for the violations set forth herein.

---

Dr. Barrett Hatches  
Chairman  
Missouri Gaming Commission

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that he caused a true and correct copy of the foregoing to be mailed, postage prepaid, this \_\_\_\_ day of \_\_\_\_\_, 2013, to:

Mr. Frank Donaghue  
Penn National Gaming, Inc.  
825 Berkshire Boulevard, Ste. 200  
Wyomissing, PA 19610

---

Dr. Barrett Hatches  
Chairman  
Missouri Gaming Commission