NATIONAL INDIAN GAMING COMMISSION

September 24, 2009

Via facsimile 717-652-8018
e-mail: db@atlantisinternetgroup.com
and First Class mail

Donald Bailey, President
Atlantis Internet Group Corp.
5601 Morning Mist Drive
Harrisburg, PA 17111-3737

RE: Casino Gateway Network

Dear Mr. Bailey:

This is in response to your request for an opinion addressing Atlantis Internet Group's Casino Gateway Network. I apologize again for the delay in issuing this opinion and for any inconvenience that may have caused. My staff and I have reviewed your detailed description of the Casino Gateway Network and its functions and engineering. We have also reviewed the additional information provided by Atlantis's gaming partners and BMM Compliance, the independent testing laboratory, and the information you provided in e-mail messages and telephone conversations. It is my opinion that the Unlawful Internet Gambling Enforcement Act (UIGEA), 31 U.S.C. §§ 5361-5367 does not prohibit the use of the Casino Gateway Network in or between licensed Indian gaming facilities to administer wide-area progressive jackpots or to play Atlantis's Bango game, bingo, or other Class II games. The Casino Gateway Network is, in other words, the kind of multi-site system the National Indian Gaming Commission addressed in Bulletin 2009-03, *The Effect of the Unlawful Internet Gambling Enforcement Act of 2006 on Wide-Area Progressive Systems and Networked, Multi-Site Bingo Games* (March 9, 2009).

By way of background, Bulletin 2009-03 set out a straightforward legal analysis in support of its conclusion that the prohibitions in UIGEA did not apply to wide-area progressive systems (WAPs) or multi-site bingo systems. UIGEA, the bulletin noted, intended no change in the status quo for legal and illegal gambling in the United States:

> No provision of this subchapter shall be construed as altering, limiting, or extending any Federal or State Law or Tribal-State compact prohibiting, permitting, or regulating gambling within the United States.

31 U.S.C. § 5361(b). Further, the bulletin said, WAPs have long been a part of legal slot-machine gambling in both commercial and compacted Class III gaming, Bulletin 2009-03 at p. 3, and in the adoption of the Indian Gaming Regulatory Act (IGRA), 25 U.S.C. §§ 2701-2721, Congress specifically contemplated multi-site bingo games and other Class II games played between facilities using telecommunications:

> In this regard, the Committee recognizes that tribes may wish to join with other tribes to coordinate their Class II operations and thereby enhance the potential of increasing revenues. For example, linking participant players at various reservations, whether in the same or different States, by means of telephone, cable, television, or satellite may be a reasonable approach for tribes to take.

S. Rep. No. 100-446, at A-9 (1988).

Beyond this analysis of UIGEA's policy, Bulletin 2009-03 stated that WAPs and multi-site bingo games were outside of UIGEA's scope because, as they are presently constructed, they fall outside UIGEA's definition of *unlawful internet gambling:*

> to place, receive or otherwise knowingly transmit a bet or wager by any means which involves the use, at least in part, of the Internet, where such bet or wager is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received or otherwise made.

31 U.S.C. § 5362(10)(A). That is, because WAPs and multi-site bingo systems use "closed, proprietary communications networks," they make no use of the Internet and do not fall within this definition. 2009-03 at 3

Bulletin 2009-03 did not elaborate further. However, a detailed, technical explanation, of how and why a closed proprietary network does not "involve the use, at least in part, of the Internet" forms the basis of my opinion here.

A closed proprietary network or, more commonly, a "private network" is separate and distinct from "the Internet" through its use of leased communication lines, Virtual Private Networks (VPNs), or some combination of the two. Communications that travel over private networks are isolated from, and not accessible to the Internet, and vice versa. This is true even though private networks may share some infrastructure with the Internet.

The easiest way to illustrate this is to borrow the analogy used in the explanation of the technology found on the *How Stuff Works* website. *See*, *Analogy: Each LAN is an Island*, http://computer.howstuffworks.com/vpn4.htm. Imagine that local area networks, or more accurately here, networked gaming equipment in a single casino, is an island in a huge ocean dotted by many other islands. The ocean is the Internet.

To travel or communicate from island to island you can take a public ferry. You travel on the ferry's schedule, and your comings and goings are visible to others traveling with you. This is the equivalent to logging on to a web site through your internet service provider at home. You have no control over how or where your traffic is routed. You have no control over the wires and routers that make up the Internet, just like you have no control over the other people on the ferry. You are exposed to potential security risks if the other passengers on the ferry decide to misbehave. *Id.*

To continue with the analogy, your island decides to build a bridge to another island so that there is easier, more secure and direct way for people to travel or communicate between the two. It is expensive to build and maintain the bridge, even though the island you are connecting with is very close. But the need for a reliable, secure path is so great that you do it anyway. Your island would like to connect to a second island that is much farther away but decides that the cost are simply too much to bear.

This is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet are able to connect the islands (casinos). Many companies have chosen this route because of the need for security and reliability in connecting their remote offices. However, if the offices are very far apart, the cost can be prohibitively high, just like building bridge across a great distance.

To solve the problem of expense, you can use a VPN, is a form of communication that utilizes secured connections over a publicly available network. While VPNs do use existing infrastructure such as the Internet to establish connections, these connections are nonetheless separate from the Internet. The term most often used to describe these dedicated connections is a "tunnel" because, conceptually speaking, these connections are isolated from their surrounding environment.

Continuing the island and ocean analogy, using VPNs is akin to giving each inhabitant of our island a small submarine. Although the submarines are traveling in the ocean along with other traffic, the inhabitants of our two islands could travel back and forth whenever they wanted to with privacy and security, invisible to all other submaries. Again, the submarines (VPNs) are separate from the ocean (Internet), yet are able to connect the islands (casinos). *Id.*

More technically, VPNs are designed to only allow access to users on either end of the connection. These are point-to-point (or casino-to-casino) connections segregated from the Internet. This level of isolation is accomplished by using various technologies that not only establish the tunnel but also how the information is transported. These include:

a) Firewall(s): A security system consisting of a combination of hardware and software that limits the exposure of a computer or computer network to attack from crackers; commonly used on local area networks that are connected to the Internet.

b) IPSec: Internet Protocol Security provides interoperable, high quality and cryptographically based security services for traffic at the IP layer, such as authenticity, integrity, confidentiality and access control to each IP packet.

c) Biometric Authentication: End user security measure that ensures user login and identification are based on unique physiological characteristics such as fingerprint identification, iris/retinal scanning, voice recognition, etc.

d) Advanced Encryption: A cryptographic algorithm that can be used to protect electronic data. The AES algorithm can be used to encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

More technically still, the Internet Assigned Numbers Authority (IANA), the central registry for Internet protocol addresses, states that addresses reserved for private networks are separate from addresses allocated to the public Internet. Internet protocol addresses (or "IP addresses") are the unique identifiers for each computer on the Internet or on private networks. They range in value from 0.0.0.0 to 255.255.255.255.

The addresses that range from 10.0.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255 are so-called "special use" addresses reserved from private networks. A private home network of three computers linked by Microsoft's Windows operating system uses addresses in the last range. VPNs typically use addresses in the first. By design, then, private networks so constructed do not have any direct IP connectivity outside of the network. *See, e.g. RFC 1918*, Network Working Group, *Best Current Practice for Address Allocation for Private Internets* (February 1996). Communications across a VPN are invisible to anyone on the Internet or, indeed, to anyone without authorized access to the tunnel. In short, at the engineering level, private networks are not "the Internet." WAPs and multi-site bingo games built on private networks do not involve "the use, at least in part, of the Internet" and are not unlawful internet gambling under UIGEA.

Reduced to its essentials, I understand the Casino Gateway Network to consist of a gaming system with single- and multi-player stations built around a client-server architecture. A library of Class II and Class III games is apparently available, along with accounting, money and credit handling, and ticketing support. More germane to the issue here, the Casino Gateway Network can link games in multiple casinos across a VPN where each casino is at the end of a secure VPN tunnel. It does so with some of the standard VPN technologies described above. According to a letter submitted by BMM Compliance, which also reviewed detailed descriptions of the system, the Casino Gateway Network

> uses Internet Protocol Security (IPSec) with a Virtual Private Network (VPN) tunnel for connections to the system. The encryption used for communication is the Advanced Encryption Standard (AES) with a key size of 256 bits. The network makes use of multiple firewalls with "deny

> all" rules and filtering by source Internet Protocol (IP) address and port number. The routers on the edges of the architecture use Access Control Lists (ACL) and the Hot Standby Router Protocol (HSRP) to control access and provide redundancy. The servers used for transactions and the database use ip-table to control packet routing.

Letter from John Golonka, Business Development Manager, BMM Compliance, to Michael Gross, Associate General Counsel, NIGC (June 23, 2009).

In short, given all of the foregoing, it is my opinion that the Casino Gateway Network is a private network. Administering a WAP and the play of Bango, bingo, or other Class II games across the network in two or more licensed tribal casinos does not involve the use of the Internet, and such uses are not prohibited by UIGEA. I make a few, final additional comments.

I note that the Casino Gateway Network contains a feature called Entertainment Plus, which as described allows a player to view the results of certain games over the Internet. It does not allow players to play these games. For example, a player who purchases chances in Atlantis's Bango Football Grid game at the casino may leave and check the results on line at home using a pair of unique identifier numbers issued at the casino, where winnings must also be collected.

This does not change my opinion about the Casino Gateway Network as a private network. It is my understanding that Entertainment Plus may only be used to check results of completed games, not to play games. Put slightly differently, the results of completed games are made available to players on the Internet using the access numbers provided. Checking the results of completed wagers on the Internet does not constitute Internet gaming or wagering involving the use of the Internet, in whole or in part, because the wagering is complete at the casino. *See* PlayAway letter from Penny J. Coleman, NIGC Acting General Counsel, to Heidi McNeil Staudemeier, Esq. (Aug. 11, 2006).

I note as well that the Casino Gateway Network can be configured to allow players to access and play casino games from their home computers. Presumably, this feature is planned to take advantage of UIGEA's so-called safe harbor provision, 31 U.S.C. § 5362(10)(C), which purports to allow the use of the Internet for intra- and inter-tribal wagers under certain conditions. I offer no opinion about the permissibility of playing from home, even if located on tribal land, or of the scope and effect of UIGEA's safe harbor as that is an open question of law about which the United States has not yet taken a position. I likewise offer no opinion on another open question, whether the Casino Gateway Network may be used to play Class III games such as slot machines.

Finally, this opinion is advisory in nature only and may be superseded, reversed, revised, or reconsidered. Furthermore, if the Casino Gateway Network fails to conform with, or differs from, the foregoing description, such differences might materially alter this opinion. It is also my understanding that the Casino Gateway Network design and documentation has been reviewed by an independent testing laboratory. This opinion should be relied upon only when an independent testing laboratory has fully tested and reviewed the Casino Gateway Network and has confirmed that its features and functions are as they have been described. Further, before the Casino Gateway Network may be offered for use in tribal casinos for the play of Class II games, it must be tested for compliance with the requirements of NIGC's Technical Standards, 25 C.F.R. part 547, by an independent testing laboratory and approved for use by the relevant tribal gaming commission.

If you have any questions, please feel free to call Michael Gross, Associate General Counsel, General Law, at 202-632-7003.

Sincerely,

Penny J Coleman

Penny J. Coleman
Acting General Counsel