Forest County Potawatomi Community

P.O. BOX 340 • Crandon, WI 54520

Testimony of Harold "Gus" Frank

Testimony of Harold "Gus" Frank
Chairman, Forest County Potawatomi Community
to the United States Senate Committee on Indian Affairs regarding
"Doubling Down on Indian Gaming: Examining New Issues and Opportunities for Success in the Next 30 Years"

October 4, 2017

Good afternoon Chairman Hoeven, Vice Chairman Udall, and other distinguished Members of the Committee. I am Harold Frank, Chairman of the Forest County Potawatomi Community (FCPC). Thank you for the invitation to appear before you on behalf of our Tribe. We appreciate the Committee's initiative in examining and preparing for the future of Indian Gaming.

The FCPC are one of eight Potawatomi bands in the United States. Our ancestral and treaty territory homelands extend from about what is now northern Indiana to the northern shores of Lake Michigan, through present day Chicago and Milwaukee.

Through revenues from a wide array of business interests, we have been fortunate enough to invest in the health, wellness, education, environment and future of our people. Among the diverse set of businesses we own are two casinos in Wisconsin and Potawatomi Business Development Corporation (PBDC).

One of the FCPC's most significant and important investments in recent years has been the modernization and enhancement of internal controls regarding cybersecurity at our casinos. It seems that every week we hear increasingly disturbing news of cyberattacks and data breaches across all industries. All organizations are vulnerable to the theft of confidential data, including casinos.

Improving controls related to cybersecurity is crucial to the future success of Indian gaming. The cost of addressing a single data breach has grown to around $4 million per incident.[1] In addition to the financial cost of being hacked, an immeasurable impact lies in the shaking of consumer confidence. The integrity and future of the gaming industry depends on mitigating the risks posed by cyber threats.

Cybersecurity Investments

Our casinos have always been compliant with the National Indian Gaming Commission's (NIGC) regulations governing internal controls, which include minimum standards for the security of sensitive data.[2] In fact, our tribal-state compact with Wisconsin requires that our minimum internal control standards (MICS) are *at least* as stringent as the Commission's regulations.

[1] (June 15, 2016). IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident. *Press Release, IBM Security.* Retrieved from http://www.prnewswire.com/news-releases/ibm--ponemon-institute-study-data-breach-costs-rising-now-4-million-per-incident-300284792.html

[2] 25 C.F.R. Part 543. The Commission updated these regulations in 2012 and 2013.

However, we recognize the wisdom of going beyond what is required by law in order to protect ourselves and our patrons from cyber theft. In these efforts, the FCPC took a large, proactive step to improve the level of cybersecurity protection at our casino enterprises by hiring a vendor to conduct a 3rd party security assessment to identify vulnerabilities and consult on any potential risks. Following that audit, our tribe invested millions of dollars to develop and implement sophisticated protections against cybercriminals. The overall takeaway was to move the network and infrastructure into high security zones through modernization. We added layers of security protection to address various threats and vulnerabilities. Some specific actions taken as a result of the assessment include:

- **Hiring a 3rd party security consultant, to assist in addressing areas of opportunity highlighted by the audit**. The FCPC hired a 3rd party security consultant to ensure that audit takeaways were thoroughly evaluated and sufficient action taken to protect from cyberattacks. The consultant has been closely involved with developing standards for IT security personnel, testing the efficacy of implemented controls and ensuring that adequate measures are taken to protect against a breach. The assistance of a 3rd party consultant has been crucial to ensuring strong controls are implemented and updated.

- **Upgrading credit card machines, ATMs and associated software to adhere to and comply with Payment Card Industry (PCI) standards.** When considering industry frameworks governing the protection of sensitive data, we found that the greatest level of protection can be achieved by adhering to PCI standards. As a result, we’ve invested in hardware that is compliant with PCI standards and offers the highest level of protection to our patrons. All credit card machines now have chip readers with encryption, per PCI requirements, whether they are customer facing or used by employees.

- **Purchasing and implementing security monitoring software to identify, isolate and address any attempts to compromise company systems.** Constant surveillance of company systems is crucial to recognizing and foiling an attack. There are numerous software-as-a-service vendors who offer products to assist in this effort. Through these products, real-time information is provided on attempts to breach company systems, allowing security personnel to take immediate action. We ensure that any vendor with which we partner is compliant with PCI standards.

- **Creating a new Security Director position, dedicated to safeguarding information technology and sensitive data**. The Security Director is a position dedicated to maintaining data security and will play an important role in developing the orientation curriculum and administering training to new and current employees. The Director will also regularly perform penetration testing, hold multiple security certifications and monitor sensitive company data.

- **Improving new hire and current employee knowledge of the risks of cyberattacks and strategies to defend against them.** As mentioned previously, the Security Director will play a large role in improving the security IQ of new and current employees. The majority of cyberattacks come through social engineering, as criminals seek to identify and manipulate key people into performing compromising actions or divulging confidential information. Ensuring that employees are aware of the strategies cybercriminals may use is an essential part of our information security plan.

- **Planning follow-up IT security audits with a 3rd party to ensure effectiveness of newly implemented security protocols.** An IT security audit involves analysis of procedure documentation, technical controls, personnel interview, physical security reviews among any other elements that affect the effectiveness of an information security program. Scheduling follow-up audits ensures that recently implemented protocols are working properly and are effective. Cybersecurity is an ongoing concern – there is no point at which an organization is done updating systems, as more sophisticated attacks are constantly being developed and executed.

Experience at Potawatomi Business Development Corporation (PBDC)

In addition to our experience operating our casinos, the Potawatomi Business Development Corporation (PBDC) was established in 2002 as the economic development and income diversification business of the FCPC.

Under the PBDC's umbrella of companies is Data Holdings, a leading data center located in Milwaukee, Wisconsin. FCPC opened the $33 million data center in May of 2013 after recognizing the growing importance and business opportunity of safely and securely storing confidential data. We wanted to be industry leaders in the data protection space, so developed the data center as the first wholesale, Tier III Enhanced facility in Milwaukee. The data center is compliant with Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) standards, which establish minimum controls for the protection of patient health data and the transmittal of credit card information, respectively. This experience has given us a unique and valuable perspective on the importance of internal control standards and the level of protection we should strive for in our other businesses, including our casinos.

In addition to owning and operating the data center in Milwaukee, the PBDC also runs Redhawk Network Security, a cybersecurity firm providing network monitoring and device support services. Redhawk partners with clients to provide them with full-time security oversight and expertise. As part of these ongoing efforts, Redhawk has been developing a modular portal to perform penetration audits on client systems and auto-generate a vulnerability report to identify and address any IT security shortfalls. Our exposure to the unique demands and ever-changing world of cyber security from a vendor's standpoint has expanded and shaped our perspective of what is required to ensure the protection of confidential information.

Recommendation

Among the greatest risks facing the future of Indian gaming is cybercrime. Proactive measures should be taken by all tribal casinos to safeguard valuable company and customer information. Indian gaming has rapidly evolving digital gaming and business systems. As these systems continue to grow, they are becoming ever more interconnected. In addition, internet-connected fixtures are becoming more common, creating additional opportunities for hackers to gain access to networks and exploit vulnerabilities.

Class II tribal gaming establishments are subject to updated NIGC regulations. However, providing guidance on recommended minimum internal control standards for class III gaming which reflect the threats of today is an important step the NIGC can take to protect against cybercrime and safeguard the future of Indian gaming.

In recent years the NIGC has consulted with tribes about drafting voluntary guidance establishing minimum internal control standards for class III gaming, which were last updated in 2006.[3] The Forest County Potawatomi Gaming Commission has responded to the NIGC's solicitation of input, encouraging the development of current and up-to-date NIGC recommended MICS.[4] As we stated in our past correspondence, the FCPC Tribal MICS are evaluated in comparison with class III MICS adopted by the NIGC as required by our compact with the state of Wisconsin. Therefore, it is in the FCPC's best interest to have current and up-to-date MICS. We continue to support the revision and updating of class III minimum internal control standards, though we recognize that the standards will be considered recommended guidelines rather than required MICS.

However, in the preparation of these guidelines, we respectfully request that a particular focus is given to properly updating the NIGC's recommended MICS regarding cybersecurity protections. Encouraging tribes to be proactive rather than reactive with cybersecurity will help protect the industry from the growing threat of cybercrime. Developing and encouraging a strong security infrastructure will help tribal organizations maintain independency and ensure long-term success.

Information security is an important safeguard that will protect tribal gaming from expanding threats in cybersecurity. Considering our status as the operator of major class III gaming facilities and our expertise in protecting and managing sensitive data for others, the Forest County Potawatomi Community would like to offer any assistance we can provide in the development of NIGC guidance regarding minimum internal control standards on cybersecurity for class III gaming.

Thank you again for the opportunity to testify before the committee today.

[3] *NIGC Consultation Topics*, Draft Guidance on the Class III Minimum Internal Control Standards, National Indian Gaming Commission, Updated December 12, 2016. Retrieved from https://www.nigc.gov/images/uploads/2016-12-12%20Consultation%20Briefing%20clean.pdf

[4] George, K. (Chairperson, Forest County Potawatomi Gaming Commission). Letter to: Stevens, T. (Chairwoman, National Indian Gaming Commission). February 7, 2011. Retrieved from https://www.nigc.gov/images/uploads/Tribal%20Consultation/Regulatory%20Review%202010-2011/ForestCountyPotawatominoicomments.pdf