



Jonodev Chaudhuri, Chairman
National Indian Gaming Commission
1849 C Street Northwest
Washington, D.C. 20240

November 13, 2017

Re: 25 C.F.R. 547.5

Grandfathered Class II Gaming
Systems

Dear Chairman Chaudhuri,

We write concerning the minimum technical standards for Class II gaming systems set forth in 25 C.F.R. 547.5. As you know, when these standards were first promulgated in 2008, the National Indian Gaming Commission ("Commission") implemented a five-year "grandfather period," temporarily exempting older gaming systems to "avoid any potential significant economic impact" of requiring immediate compliance.¹ In 2012, before the first five-year grandfather period was about to expire, the Commission extended the grandfather period an additional five years because of the economic downturn which required "keeping a grandfathered system on the gaming floor for a longer period of time."²

As the expiration of this second set of five years approaches, we understand there has been lobbying for yet another extension, this time a permanent one. The Commission should reject any additional extension, for multiple reasons.

First, as the Commission is aware, it is in the best interest of the tribes and the public to have a uniform minimum security standard across all Class II machines. The Commission itself sets out as its first principle to "address and mitigate activity that jeopardizes the integrity of Indian gaming,"³ fulfilling the request of Congress through IGRA that Indian gaming be "conducted fairly and honestly by both the operator and players."⁴ The security risks posed by these obsolete machines threaten the integrity of Class II gaming, and those risks are only increasing with time. As the Commission has noted, the "technical standards are intended to ensure the integrity and security of class II gaming and accountability of Class II gaming revenue," and "include minimum requirements that the Commission believes, in its judgment, are appropriate and consistent with its Federal regulatory oversight mission."⁵

Hacking and security breaches have become commonplace, even within the Indian

¹ Minimum Technical Standards for Class II Gaming Systems and Equipment, 77 Fed. Reg. 58,475 (Sept 21, 2012) (codified at 25 C.F.R. pt. 547)

² Id.

³ National Indian Gaming Commission, Our Mission. <https://www.nigc.gov/commission/principles-and-priorities>. Accessed October 16, 2017.

⁴ 25 U.S.C. 2702

⁵ Technical Standards, 82 Fed. Reg. 45,229 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

gaming industry, and many of them are specifically targeted at older machines because they lack the protections of the minimum technical standards. As the Commission has noted, not only is the risk very real, but it increases over time “as technology advances and grandfathered machines remain static . . .”⁶

Second, requiring compliance will have little to no negative economic impact on the Tribes. In contrast to when the Commission last extended the grandfather period for five years because of concerns about the “economic downturn,” Indian gaming has never been stronger. We are now on the 7th straight year of growth for Indian gaming nationwide, and on the heels of the best year ever, where revenue from Indian gaming was at an all-time high in 2016 of \$31.2 billion.⁷

The Commission’s decision to allow grandfathering was based on a 2008 study by Dr. Alan Meister (“Meister Report”),⁸ which predicted dire economic consequences of requiring immediate compliance with the minimum technical standards. But these predictions have not held up over the last nine years. Thousands of new and compliant Class II gaming systems have been placed in service since 2008, and Class II gaming thrives. The technology to make compliant machines has already been developed over the past nine years, so there will be no additional development costs. And to the extent there are still costs of bringing grandfathered machines into compliance, the tribes will not see them; such costs would be borne by the manufacturers, who nearly always retain ownership of the gaming system and share revenue with the tribal casino operator.

Third, a permanent extension of the grandfather period would be anti-competitive in at least two respects. An extension would harm newer manufacturers of Class II gaming machines, thereby putting this regulation at risk of being found arbitrary and capricious. As compliant machines cost more to manufacture than non-compliant machines, the Commission’s grandfather period has created, and continues to enable, an unequal playing field, granting the manufacturers of older Class II machines a competitive advantage against newer entrants to the market. Any more extensions would cement the selective applicability of this regulation as unlawfully arbitrary and capricious.

Fourth, a permanent extension would qualify the Class II regulations under 5 U.S.C. 804 (the Small Business Regulatory Enforcement Fairness Act) as a Major Rule in at least two ways. First, because the economic justification for the grandfathering claims an economic impact of between \$1.2 billion and \$3.7 billion, far in excess of the \$100 million threshold under the Act, and second, because permanent grandfathering would have a significant adverse effect on the ability of domestic entities to compete with foreign entities, who own a majority of the grandfathered machines.⁹

Fifth, the Commission’s proposed justification for the removal of the sunset provision is

⁶ *Id.*

⁷ See included report by Sage Policy Group, Inc.

⁸ *The Potential Economic Impact of the October 2007 Proposed Class II Gaming Regulations*, available at: <https://www.nigc.gov/images/uploads/NIGC%20Uploads/proposedregs/MeisterReport2FINAL2108.pdf>

⁹ Eilers-Fantini Quarterly Slot Review, 1Q CY17, pg. 14

both unnecessary and at odds with the stated purposes of the regulations of 25 C.F.R. 547. The Commission has justified cementing the grandfathering on the grounds that there is an alternative method of ensuring their security. However, the regulations *already contain* a process to create and approve an alternative standard. Overriding that process undermines the authority granted to the TGRAs to create such standards and present them to the NIGC for approval. And ultimately, the Commission's proposed alternate standard for all grandfathered machines does not, and cannot, meet the standards the Commission itself outlined for all proposed alternate standards.

Finally, there may be serious, unintended ripple effects from extending grandfathering any further. Outdated machines are a serious security risk to themselves, to other compliant machines on the same floor, and to the casino's internal systems. Yet the consequences of such a breach would be even greater than normal due to the nature of the Class II market, which is based on a loyalty system with many readily available and very similar alternative products but with low transfer between brands. In the event of such a highly visible and disruptive security breach in the industry, there is a small but significant chance that those in the Department of the Interior overseeing the NIGC may wish to reconsider allowing Class II gaming to retain its significantly softer regulatory environment when compared to Class III gaming.

For the foregoing reasons, we urge the Commission to remain unwavering, and allow the grandfather period to expire as originally intended. This will result in the equal treatment of all gaming machine manufacturers, and benefit the public and tribes by ensuring that *every machine* meets a minimum standard of security and integrity.

I. Regulatory History

In 2003, the Commission decided that “it is in the best interests of Indian gaming to adopt technical standards,” governing Class II gaming machines to ensure their security and integrity. At that time, no such standards existed, and patrons had to rely solely on inconsistent tribal regulations to ensure the integrity of their gaming experience. In proposing the technical standards, the Commission decided to “remedy that absence.”¹⁰ The Commission took a variety of steps in preparation for proposing rules, including conducting over 300 separate government-to-government consultation meetings with various tribes and their representatives, establishing a joint Federal-Tribal Advisory Committee to assist in the creation of the regulations and, after the regulations were written, conducting lengthy notice and comment periods to allow interested parties an opportunity to discuss any objections.¹¹

At that time, the Commission determined that, “it [was] in the best interest of Indian gaming to adopt technical standards that govern[ed] the implementation of ... technologic aids used in the play of Class II games because no such standards currently exist[ed].”¹² The Commission further stated that these standards, “[sought] to... ensure that the integrity of Class II games... [was] maintained; that the games... [were] secure; and that the games... [were] fully

¹⁰ Technical Standards for “Electronic, Computer, or Other Technologic Aids” Used in the Play of Class II Games, 71 Fed. Reg. 46,337 (Aug. 11, 2006) (codified at 25 C.F.R. pt. 547)

¹¹ *Id.* at 46,337

¹² Technical Standards for Electronic, Computer, or Other Technologic Aids Used in the Play of Class II Games, 72 Fed. Reg. 60,508-9 (Oct. 24, 2007) (codified at 25 C.F.R. pt. 547)

auditable,” in order “to ensure the security and integrity of Class II games.”¹³

While the proposed rule required all gaming systems to meet the new standards, after hearing concerns from manufacturers about the potential for negative economic consequences of requiring an immediate change, the Commission requested a study of the regulations’ economic impact. Dr. Alan Meister’s resulting report assumed that Class II games would “be slower, more cumbersome, and less appealing than what is being operated in Class II gaming facilities today [in February].” *See* Meister Report at 38. The study predicted a dire economic future: billions in lost revenue, and thousands of lost tribal jobs.

Because of these concerns, the Commission’s final rule included a “grandfathering period” for older machines. Machines manufactured before November 10, 2008 had five additional years to become compliant.

In 2011, the Commission undertook a complete review of its regulations. Once again, the Commission consulted with tribes, established a Tribal Advisory Committee to allow tribal representatives input into the initial draft of the proposed rule changes, published a discussion draft of the proposed rule changes, and after publishing notice in the Federal Register, held an extended notice and comment period on the proposed rule changes.¹⁴ Throughout this process, “[m]ore than any other topic, [the grandfathering period] has been the subject of long deliberation and analysis.”¹⁵ Though it received numerous comments against the sunset provision of the grandfathering period, the Commission opted to retain it.

The Commission extended the original five-year grandfathering period to ten years to “Balanc[e] those economic needs [of the tribal gaming operations] against a risk that increases as technology advances and grandfathered machines remain static . . .”¹⁶ Specifically, the Commission stated that the “lack of a major incident in the past does not mean that the grandfathered Class II gaming systems pose no risk to patrons and the gaming operation,” citing for an example the minimum security requirements of §547.15.¹⁷ That risk remains more pressing as ever, but the benefit it was supposed to protect, the economic needs of the tribes in the face of the predicted economic recession the Commission anticipated compliance would trigger, has never materialized. Tribal gaming continues to experience significant growth in revenue even after thousands of compliant machines have been developed and placed.

II. Discussion

For the following reasons, we urge the Commission to allow the current grandfathering period to expire, as the Commission always intended it to.

¹³ *Id.*

¹⁴ Minimum Technical Standards for Class II Gaming Systems and Equipment, 77 Fed. Reg. 58,473 (September 21, 2012) (codified at 25 C.F.R. pt. 547)

¹⁵ *Id.* at 58,475

¹⁶ *Id.*

¹⁷ *Id.*

A. *The public and tribes are best served if all machines adhere to minimum security and integrity requirements.*

As the Commission is aware, a uniform minimum standard of security is in the interest of both the public and the tribes themselves. The integrity and security risks posed by these old, noncompliant machines—risks which drove the Commission to pass the minimum technical standards in the first place—is only increasing over time. The Commission believed that the Class II machines in question were out of date in 2008. Nearly 10 years have passed since then, and while it seems unnecessary to say, the Class II machines have only gotten older and even more out of date, while threats to the industry have grown.

Hacking and security breaches have gone mainstream in this country, affecting individuals, companies, and all branches and levels of government. The Indian gaming industry is not immune. The question is no longer if an attack will occur, but when. It is only a matter of time before Class II machines are the victims of an enormous security breach or fraud. As the grandfathered machines have the lowest security thresholds, they are the most vulnerable and will likely be the first targets of attack.

Specifically, we refer to the attached security analysis prepared by Conquest Security,¹⁸ which notes that "security risks are the number one danger of older technology." The report goes on to describe the general dangers of outdated firmware, operating systems, hardware, and more, and continues to describe many of the security vulnerabilities mitigated by each of the Minimum Technical Standard's requirements. We also point out that such risks are not simply theoretical.

In 2014 several Missouri casinos' Aristocrat Legacy Mark VI machines (whose subsidiary Video Gaming Technologies, incidentally, we understand to be strongly against the sunset provision) were successfully targeted by a team of Russians, who stole tens of thousands of dollars, and who have already circumvented the methods used to detect them in that instance.¹⁹ It turns out that Novomatic, Atronic, and Mega Jack machines have been targeted by similar, still poorly understood methods as far back as February of 2011,²⁰ which methods impacted the hold percentage at 50% to 400%.²¹ And even now, six years after the discovery of this, one of many vulnerabilities of older machines, any grandfathered machines remain unchanged, and the NIGC proposes to ensure that these known and unknown vulnerabilities are never removed.

In discussing these breaches, Darrin Hoke, Vice President of Operation Protection at L'Auberge Du Lac Hotel and Casino,²² said in a report entitled "Russian Slot Cheating Team: A Reference Guide" that the targeted machines use "relatively older technology" leaving "any number of methods" to cheat them.²³ He noted the likelihood that the intrusions made "use of a

¹⁸ *Class II Gaming Systems Risk Analysis Report*, Conquest Security, November 13, 2017.

¹⁹ Koerner, Brendan. *Wired. Russians Engineer a Brilliant Slot Machine Cheat—and Casinos have no Fix*. February 6, 2017. Available at: <https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/>

²⁰ Darrin Hoke, *Russian Slot Cheating Team: A Reference Guide*, 1. July 15, 2014. See Attached copy.

²¹ *Id* at 2.

²² As stated on his linkedin profile, accessible at <https://www.linkedin.com/in/darrin-hoke-203925/>

²³ *Id* at 2.

wireless technology,”²⁴ the security of which, not coincidentally, is covered by the Minimum Technical Standards²⁵ which grandfathered machines are exempted from.

When asked to comment, Aristocrat stated that it was “unable to identify defects in the targeted game,” and told its customers in a Security Bulletin that it had “not identified any weaknesses in our software that would make these games susceptible to unlawful activity.”²⁶ The specific targeting of these “older machines” running 50 Lions, 100 Lions, Hearts of Gold, Miss Kitty, Pelican Pete, Star Drifter, and Wild Panda indicates that these weaknesses do, in fact, exist.²⁷ And worryingly, Aristocrat reassured their customers that, despite the “quite sophisticated”²⁸ methods used to compromise their machines, there was no impetus to change because “all Aristocrat products are built to and approved against rigid regulatory standards” and that “these standards include strict adherence to all aspects affecting the security and integrity” of their games.²⁹

These reassurances are, since Aristocrat’s acquisition of VGT and its many grandfathered games, no longer true, but more to the point, the public and the tribes continue under the mistaken belief that the NIGC has applied the Minimum Technical Standards to all Class II games. The NIGC has exempted many of Aristocrat’s, and others,’ machines from the majority of the regulatory standards, and has failed to inform the public of doing so to allow them to protect themselves from these vulnerabilities. It is in the interest of the public to ensure that the safety standards are applied to all Class II gaming, but we note that, Aristocrat’s resistance aside, it is actually in the interest of those with grandfathered machines to avoid becoming a target by complying with the, we stress, *minimum* technical standards decided upon by the Commission almost a decade ago.

Allowing for the permanent exemption from security and safety requirements in the face of an acknowledged, *growing* security risk, even in light of evidence of actual targeting of those vulnerabilities, would go against the Commission’s purpose in creating the minimum technical standards to “ensure the integrity and security” of class II games and is an abnegation of the Commission’s duty to protect both the Indian Tribes and the public.

Moreover, allowing the continued use of the grandfathered systems perpetuates the regulatory nightmare caused by the initial grandfathering. The Commission provided 10 years to retire these machines or bring them into compliance, yet there is no evidence this has been done. There is no way to know how many pre-2008 Class II machines remain in the marketplace, as per the 2008 Meister report, there were 43,179 machines distributed across the 15 states that had Class II gaming in 2008,³⁰ but the regulations allowed any stored, non-compliant machines to qualify so long as they were registered. The list of registered machines has never been made public, and with the large surge in purchases just before the cutoff date, there could at this

²⁴ *Id* at 2.

²⁵ 25 C.F.R. pt. 547.15(b)

²⁶ Aristocrat. *Security Bulletin*. PN-14-020, July 16, 2014

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ Alan Meister, The Potential Economic Impact of the October 2007 Proposed Class II Gaming Regulations 26-37 (2008) [hereinafter Meister, Economic Impact].

moment be anywhere between 5,000 and 50,000 grandfathered games on casino floors. We also note that the Commission proposes to make all such “sensitive” compliance information immune from Freedom of Information Act discovery,³¹ thus hiding from both the public and the industry which machines are potentially dangerous to them. The Commission may be willing to cement long-term risks to the public for the benefit of a select few manufacturers, but if it is going to sidestep its principle to protect the “health and safety of the public,” at the very least it should allow a concerned public to have access to the information it needs to protect *itself* from these machines.

However many grandfathered machines there may be, any machines produced after 2008 would have to be compliant with the regulations. Replacing 4,300 machines a year over the past 10 years should have been easy to accomplish, particularly as only California and Oklahoma had more than 4,300 noncompliant machines in operation within those 15 states in the first place.³² Unless the manufacturers have completely ignored the 2008 regulations, the number of non-compliant machines must surely be lower today than it was when the grandfathering was passed. Thus, the burden of compliance should have decreased as well.

Yet despite these increased risks and lower compliance costs, grandfathering, which was intended to help manufacturers become compliant, has not worked, and manufacturers have taken advantage of the Commission’s helpful intentions. To fulfill its regulatory role, the Commission should end the grandfathering and require all Class II gaming systems to be brought into compliance with the minimum technical standards.

B. Requiring compliance will not negatively impact tribes.

There is no better time than now for the Commission to require Class II gaming machines to meet the its minimum technical standards. The Indian gaming industry is experiencing record expansion.³³ In 2015, growth more than doubled the already impressive expansion of the industry in 2014, setting a record.³⁴ Revenues were at an all-time high of \$30.5 billion, with a value to the U.S. economy that exceeds \$100 billion.³⁵ Indian gaming’s recent growth more than doubled the growth of the U.S. economy, with a 5.5% improvement in 2015, compared to the U.S. economy’s 2.5% growth in gross domestic product over the same period.³⁶

In addition to the industry’s boom minimizing the impact of any compliance costs, the costs themselves are substantially lower now than forecasted a decade ago in the Meister Report. Moreover, such costs have been borne by the manufacturers of gaming machines, not the Tribes. And with thousands of compliant gaming machines developed and placed since 2008, manufacturing and operating compliant machines is clearly feasible. The non-tribe owners of the non-compliant machines have both the technology and resources to bring all non-compliant gaming machines into compliance prior to the November 18, 2018 deadline.

³¹ Technical Standards, 82 Fed. Reg. 45,230-45,231 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

³² *Id.*

³³ Alan Meister, Casino City’s Indian Gaming Industry Report 13 (2017). [Hereinafter Casino City’s Industry Report]

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

The 2008 Meister Report predicted enormous costs and dire economic consequences for the tribes if the Commission required immediate compliance with its minimum technical standards. These predictions included:

- Lost gaming revenue of \$1.2 billion each year³⁷
- Lost non-gaming revenue of \$126.9 million annually³⁸
- Increased capital, deployment, and compliance costs of \$347.9 million, which “would be borne by the tribes”³⁹
- Lost tribal member jobs totaling 7,890 per year, as a result of all the lost revenue mentioned above⁴⁰

Based on these ominous predictions in the Meister Report, it is understandable that the Commission decided to implement the grandfather period and allow more time to meet the minimum technical standards.

However, with the benefit of history we can now see that the assumptions supporting these predictions were simply incorrect. Chief among these predictions—and the one that supported the prediction for \$1.2 billion in lost gaming revenue annually—was the Report’s assumption that Class II machines that met the minimum technical standards would “be slower, more cumbersome, and less appealing than what is being operated in Class II gaming facilities [at that time].”⁴¹

As the Commission knows, the opposite has turned out to be true. Instead of being “slower, more cumbersome, and less appealing,” the new, compliant Class II machines today are faster, sleeker, and arguably more appealing than the old, non-compliant machines on the floor in 2007 and early 2008.

With just this one incorrect assumption, nearly the entire house of cards built in the Meister Report comes crashing down. Certainly, the industry would no longer lose \$1.2 billion each year due to “slower, more cumbersome, and less appealing” class II machines. Nor would there be lost non-gaming revenue of \$126.9 million annually, as that number was based on the lost gaming revenue. And the loss of nearly 8,000 tribal member jobs each year would also never happen, as that was based on the non-existent lost revenues.

But there are still more false assumptions in the Meister Report. The Report predicts, incorrectly, that it would cost nearly \$90 million to develop compliant Class II gaming software, and that these costs would be passed on from the manufacturers to the tribes. That has not happened. The software to make compliant Class II games has already been developed, and the costs of developing has already been borne, by the manufacturers, as thousands of compliant

³⁷ Meister, Economic Impact at 50

³⁸ *Id.* at 52

³⁹ *Id.* at 56

⁴⁰ *Id.* at 58

⁴¹ *Id.* at 38

machines have been placed into service since 2008. The tribes know that it costs them no more to have a compliant machine on their floor than it does to have a non-compliant one.

Indeed, since the tribes lease virtually all Class II gaming systems from the manufacturer, which retains ownership of the gaming system in exchange for a revenue share with the tribal casino operator, there are no increased costs whatsoever that are “borne by the tribes” for bringing machines into compliance. This means the remaining “capital, deployment, and compliance costs,” which the Meister Report claimed would be approximately another \$260 million, would not be borne by the tribes.

Moreover, the Commission has affirmed repeatedly for the last decade that the Minimum Technical Standards “will not cause a major increase in costs or prices” for the industry, the region, or local government agencies, both explicitly, and in its declaration that the regulations do not qualify as a Major Rule under the Small Business Regulatory Enforcement Fairness Act.⁴² A level playing field with 100% compliant Class II gaming machines allows healthy competition among manufacturers to lease the Class II games on a competitive basis and protects the tribes from the more dominant manufacturers with many older and non-compliant gaming machines. This level playing field would make it, at worst, cost-neutral for the tribes to have compliant or non-compliant class II machines, and at best, offer them cheaper, more competitive lease agreements.

C. Another extension would unfairly, and unlawfully, benefit manufacturers of older machines.

Permanent extension of the grandfathering provision would have anti-competitive effects. The Minimum Technical Standards contain a number of rules that require higher quality components (both in terms of the physical construction⁴³ and hardware-software interaction⁴⁴), updated and improved software,⁴⁵ and some additional hardware components.⁴⁶ Not surprisingly, these improvements are associated with costs, both in terms of retroactively improving and upgrading machines to be able to comply, and in terms of newly constructed machines. Our calculations estimate that the price for compliance is \$2,966.00 higher *per machine* to comply with the regulations,⁴⁷ to say nothing of the millions of dollars spent developing the technology required and paying for lab certifications of the compliant technology. As a result, manufacturers who comply with the rules are being economically punished, and manufactures who do not comply reap the rewards of the Commission’s lenience.

And while this itself generates a competitive advantage, the problem is exacerbated by the widespread existence of grandfathered machines. Many manufactures choose their materials

⁴² Technical Standards, 82 Fed. Reg. 45,231 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

⁴³ e.g. 25 C.F.R. pt. 547.7(b) that requires the entire gaming system to be constructed of materials such that it is immune to human electrostatic discharge

⁴⁴ e.g. 25 C.F.R. pt. 547.7(a)(1) that requires that non-standard printed circuit boards bear unique and updated identifiers reflecting revisions to the board and software

⁴⁵ e.g. 25 C.F.R. pt. 547.8(d) that requires an additional Last Game Recall functionality

⁴⁶ e.g. 25 C.F.R. pt. 547.7(e) that requires a secure and locked area built into the cabinet to store all components that read account access media

⁴⁷ See attached spreadsheet entitled “Cost of Compliance vs. Non-Compliance”

based on the fluctuating market price, which in turn is driven by demand. When most manufacturers want the same standard of materials (such as when required by a regulation), the demand increases, and the market responds by producing more, and cheaper, products. However, when a majority, or even a large minority, of the market continues to use inferior materials, the price for compliant materials remains high, placing the already advantaged non-compliant machines in an even more advantageous position. In this way, the existence of grandfathered machines makes it more difficult to comply with the Commission's regulations.

This anti-competitive effect is made worse by the nature of the market, which requires heavy up-front capital investments in terms of building the machines themselves and applying for all the relevant licenses, as well as the costs of certification from Independent Gaming Labs, in return for lower but long-term returns, making an already high barrier to entry even higher. Once again, this effect is made worse by the presence of cheaper, non-compliant machines in the marketplace, which drive down the demand both for more expensive (to the manufacturer) new machines as well as for replacements, as manufacturers push old machines past their normal lifespan to avoid replacing them with more expensive, compliant machines.

Due to this cost differential, the Commission would effectively be granting a competitive advantage to those with vulnerable machines. It would allow manufacturers to shift the costs of complying with the regulations, the very same regulations with which all others in the industry must comply, from themselves to the consumer in the form of security risks. This unequal treatment of manufacturers is the definition of arbitrary and capricious, and places the regulation at risk.

D. Removing the sunset provision would qualify both the Minimum Technical Standards as a whole, and the proposed modification individually, as Major Rules under the Small Business Regulatory Enforcement Fairness Act.

The Commission states that the proposed rule does not qualify under 5 U.S.C. 804 (the Small Business Regulatory Enforcement Fairness Act) as a major rule. However, such a statement is inconsistent with the rationale upon which the Commission relies in promulgating this proposed rule.

In proposing and adopting the minimum technical standards in 2008, the Commission stated that the proposed rules do not qualify as a major rule under 5 U.S.C. 804 because they do "not have an effect on the economy of \$100 million or more," and because they "will not cause a major increase in costs or prices" for the industry.⁴⁸ After concern was expressed during the notice and comment period, the Commission created the initial, and later second, grandfathering periods largely based on accepting the Meister Report, which warned of between \$1.2 billion and \$3.7 billion in lost revenue as a direct result of the regulations.

It is not possible that the Minimum Technical Standards do "not have an effect on the

⁴⁸ Minimum Technical Standards for Class II Gaming Systems and Equipment, 77 Fed. Reg. 58,479 (September 21, 2012) (codified at 25 C.F.R. pt. 547)

economy of \$100 million or more,” and “will not cause a major increase in costs or prices”⁴⁹ while simultaneously requiring a grandfathering provision to relieve up to \$3.7 billion in lost revenue. The Commission cannot believe and rely upon the Meister Report without making the entire Minimum Technical Standards a major rule, contradicting its earlier statements in the Federal Register, and potentially subjecting its decision to judicial review under the Small Business Regulatory Enforcement Fairness Act.

Likewise, the Commission states that the new proposed rule removing the sunset provision does not qualify as a major rule because it will not “have a significant adverse effect on competition, employment, investment, productivity, innovation, or the ability of the enterprises, to compete with foreign based enterprises.”⁵⁰ This may have been true in 2008, when the initial rules were proposed, but with the proposed removal of the sunset provision it is no longer the case.

Specifically, we refer to the fact that the vast majority of grandfathered machines are now ultimately owned by foreign enterprises, and allowing foreign entities a competitive advantage (as discussed above) through a permanent exclusion from safety and security requirements has a significant, adverse effect on the ability of domestic entities to compete with them. As of March 31, 2012, 11% of the machines leased to tribes in North American were provided by foreign controlled manufacturers.⁵¹ After a flurry of acquisitions, notably that of VGT by Aristocrat in 2014 and IGT by Gtech S.p.A in 2015, that number has soared. As of March 31, 2017, foreign entities control 63% of machines leased to tribes in North America.⁵²

The Commission cannot rely upon the Meister Report without making the Minimum Technical Standards, both as originally enacted and as proposed here, into Major Rules under the Small Business Regulatory Enforcement Fairness Act. Nor can it ignore the changing realities of the industry and unknowingly offer special protections to foreign entities, offering competitive advantages over their domestic counterparts, without abiding by the statutory requirements for doing so.

E. The Commission’s rationale for removing the sunset provision is both insufficient and at odds with the stated purposes of the regulations of 25 C.F.R. 547.

The Commission states that removal of the sunset provision is “justified provided that 2008 Systems are subject to additional annual review by the TGRA.”⁵³ However, the proposed changes are unnecessary because the regulations already contain a process for creating and implementing such an alternative method of ensuring the safety and integrity of Class II gaming.

As written, the regulations in 25 C.F.R. 547.17 allow a TGRA to create an alternative standard, present it to the NIGC for approval, and allow non-compliant machines to become

⁴⁹ *Id.*

⁵⁰ Technical Standards, 82 Fed. Reg. 45,231 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

⁵¹ Eilers-Fantini Quarterly Slot Review, 1Q CY13, pg. 7

⁵² Eilers-Fantini Quarterly Slot Review, 1Q CY17, pg. 14

⁵³ Technical Standards, 82 Fed. Reg. 45,229 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

compliant by adhering to that standard. There is no need rewrite the regulations to accomplish a goal that can easily be done through them, particularly when not doing so produces so many other problems.

Moreover, overriding the already existing means of creating an alternative standard undermines the authority granted by the NIGC to the TGRAs. In effect, this proposed rule merely serves to bypass the TGRA's creation of the standard, the TGRA's determination that the alternate standard "will achieve a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace," and the TGRA's proposal of the alternative to the Chair of the NIGC.⁵⁴ Instead, by altering the regulations instead of following them, the Commission effectively dictates a new standard of annual review by the TGRA *to* the TGRA, and replaces the TGRAs expertise in creating such an alternative with the advice of a single commenter.⁵⁵

More egregious still, it completely strips the TGRA of the authority granted to it in the regulations when the Commission noted that these "are *minimum* standards and a TGRA may establish and implement *additional* technical standards" (emphasis added) that do not conflict with the regulations.⁵⁶ If under the assault of hacking attempts a new vulnerability is discovered, the TGRAs will be powerless to intervene with new protections for the oldest, most vulnerable machines, because those machines are exempted from any technical standards whatsoever.

This would be less worrisome if the Commission's imposed alternative standard were sufficient. However, even if the Commission's proposed alternative standard were properly created by a TGRA, which made the appropriate determinations and presented it to the Chair of the NIGC, the Chair would be unable to approve the "additional annual review"⁵⁷ standard because it fails to meet the criteria laid out in the regulations. The Commission's current rules found in 25 C.F.R. 547.17 require that any alternative standard achieve the same level of security and integrity as those of the initial standards.⁵⁸

The Commission's proposed annual reviews may be able to *detect* intrusions or security breakdowns (though how such a review would be helpful when the machines are not required to record intrusion attempts⁵⁹ remains an open question), but hardware and software security provisions already present in the Minimum Technical Standards are designed to *prevent* such breaches, not simply detect them. Such an alternative standard cannot possibly fulfill the requirements set forth in the regulatory language, and by supplanting the regulations already in place for a decade with an inadequate alternative for a select set of the most vulnerable machines, the Commission fails to meet its principles to "swiftly act" on anything that jeopardizes health and safety, to engage in "sound regulation," and to "address and mitigate activity that jeopardizes the integrity of Indian gaming,"⁶⁰ and openly flouts its third

⁵⁴ 25 C.F.R. pt. 547.17(a)-(b)

⁵⁵ Technical Standards, 82 Fed. Reg. 45,230 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

⁵⁶ Minimum Technical Standards for Class II Gaming Systems and Equipment, 77 Fed. Reg. 58,480 (September 21, 2012) (codified at 25 C.F.R. pt. 547)

⁵⁷ Technical Standards, 82 Fed. Reg. 45,229 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)

⁵⁸ 25 C.F.R. pt. 547.17(a)-(b)

⁵⁹ 25 C.F.R. pt. 547.15(d)

⁶⁰ National Indian Gaming Commission, *Our Mission*. <https://www.nigc.gov/commission/principles-and-priorities>. Accessed October 16, 2017.

Foundational Priority of “Staying ahead of the technology curve”⁶¹ by allowing decade-old machines to “remain static.”⁶²

F. There may be serious, unexpected ripple effects for the Class II gaming industry if the grandfathering period is extended indefinitely.

The rationale for the grandfathering periods was that the policy was a compromise “balancing . . . economic needs against a risk that increases as technology advances and grandfathered machines remain static.”⁶³ As discussed above, the economic justification for this policy is flawed, increasing the relative cost of grandfathering in this balancing analysis. Yet while the supposed economic loss the policy was to protect against is completely absent, the risks associated with continuing the grandfathering exemptions continue to climb, further militating against the exemptions.

Economic risk to the manufacturers that lease grandfathered machines, the casinos that operate them, and the patrons that frequent them, grow exponentially with each year that passes as the grandfathered EGMs become a greater and greater outlier in the market, drawing the attention of potential hackers as the easiest targets available, and courting security breaches and possibly accompanying lawsuits. And this is to say nothing of the less-easily-measurable risks, such as the loss of trust of patrons when they discover that they have been playing machines that were deemed unsafe and insecure for their fellow customers ten years ago (or longer), or discovering that their favorite venue or game has been targeted by criminals.

This risk is even more pronounced in a market based on the Loyalty business model, where there are very similar alternative products readily available, but transfer between brands is relatively low. In this type of market, consumer retention is based on the association of previous, positive emotional experiences with a particular brand. Such experiences are strong, but can be overshadowed by a newer, strongly negative experience, leading to feelings of betrayal and permanent abandoning of a brand or manufacturer. The resulting long-term loss of market share can be very difficult to recover from.

Such a potential high-visibility security breach would also court greater legislative intervention and higher mandatory standards. Currently the Class II market functions in significant part because it has a lower regulatory burden than Class III games, as well as immunity from Compact Fees by the Tribes. If the regulatory measures allowed by the governing body, in this case the NIGC, were to allow such insecure machines to suffer a major break in, it could potentially trigger a re-evaluation of the legitimacy of Class II gaming's significantly softer regulatory environment by the NIGC's superiors in the Department of the Interior.

The longer grandfathered machines are allowed to remain in place, the greater the risk of significant direct loss by both the manufacturers and the casinos, an accompanying catastrophic loss in the marketplace, and possibly even a shakeup of the Class II market itself.

⁶¹ *Id.*

⁶² Technical Standards, 82 Fed. Reg. 45,229 (September 28, 2017) (to be codified at 25 C.F.R. pt. 547)


⁶³ *Id.*

III. Conclusion

The Minimum Technical Standards were promulgated with an open acknowledgement that both the public and the tribes are best served if all machines adhere to security and integrity requirements. For nearly the past decade, the Commission has exempted those machines most vulnerable to attack on the rationale that huge economic costs would ensue from compliance, despite its own repeated statements that no such costs would materialize and that no costs would be passed on to the tribes. It now proposes to make such security flaws permanent, granting a competitive advantage in the industry to foreign entities despite its claims to the contrary, and replacing even the *minimum* technical standards with an annual review that would not pass even the loose requirements of its own regulations. The proposed rule violates the NIGC's principles and potentially opens itself to the direct intervention of the courts in its affairs.

All of these problems will be avoided if the Commission instead chooses to do nothing. If the sunset provision is allowed to expire as it was meant to, the Commission will have succeeded in its goal to create a uniform standard for all of Class II gaming, ensuring the safety and protection of patrons, the tribes, and manufacturers alike. There will be no artificial advantages to certain manufacturers, especially foreign-owned, at the expense of our public's safety. There will be fair competition, continued innovation, and investment in Class II gaming. And as an added benefit, the administrative and recordkeeping costs of tracking each grandfathered machine, of ensuring that each modification makes each machine more compliant, and detailing where on the road to compliance each machine lies, will be a thing of the past. Instead, there will be a single, simple, uniform standard fairly applied to everyone. The Commission has bent over backwards to help lagging adherents long enough. It is time to enforce the rules agreed upon in 2003.

For these reasons, we respectfully submit that the grandfathering provision in 25 C.F.R. 547.5 should run its course on November 10, 2018.

A handwritten signature in black ink, appearing to be 'RD', is written over a solid horizontal line.

Richard Dreitzer

The Coalition for Fair Gaming

Coalition for Fair Gaming, LLC

Class II Gaming Systems Risk Analysis Report

November 12, 2017

Prepared by:



Conquest Security, Inc.
267 Kentlands Blvd., #800
Gaithersburg, MD 20878
www.conquestsecurity.com

Confidential

INTRODUCTION

The Indian Gaming Regulatory Act of 1988 (IGRA) established the various classes of gaming. Bingo and similar games were classified under this regulation as “Class II”. This included electronic systems that simulate these games. The electronic games are sophisticated and mimic the Las Vegas (Class III) style slot machines while still based on the game of Bingo.

Minimum technical standards entitled “Technical Standards for Electronic, Computer, or Other Technologic Aids Used in the Play of Class II Games” (25 CFR 547) were published by the National Indian Gaming Commission (NIGC) on October 10, 2008. The purpose of this regulatory requirement was to assist tribal governments, tribal gaming regulatory authorities, and operations in ensuring the integrity and security of Class II games and gaming revenue. The Commission understood that existing Class II gaming systems likely did not meet all the requirements of the Technical Standards. To avoid any potentially significant economic and practical consequences of requiring immediate compliance, the Technical Standards implement a five-year “grandfather period” for existing gaming systems. This requirement specifically stipulated that all Class II machines must be compliant or removed by November 10, 2013.

On September 21, 2012, the commission updated its regulatory requirement and published “Minimum Technical Standards for Class II Gaming Systems and Equipment”. This revision was critical to tribal gaming regulators as the standards provided much needed updates to the control regulations, which had fallen behind technology, and were intended to ensure the integrity of Indian Gaming is upheld. The grandfather clause was extended for Class II gaming systems manufactured before November 10, 2008 from November 10, 2013, to November 10, 2018.

On September 28, 2017, the NIGC proposed to amend the minimum technical standards for Class II gaming systems and equipment. The proposed rule removes the deadline by which qualified grandfathered machines built prior to November 10, 2008 must be compliant with the full technical standards.

This paper shows that the minimum technical requirements are essential controls for ensuring the integrity and security of Class II gaming systems. The paper explains the risks mitigated for each control defined in 25 CFR 547. Gaming systems that do not comply with these regulatory controls are significantly at risk of attack and compromise due to the absence of controls on obsolete hardware, firmware, operating systems, and software.

THE RISKS AND DANGERS OF OUTDATED TECHNOLOGY

Many of the normal economic forces that drive technology and security updates in the business world do not work as effectively in the Class II gaming industry.

Computer hardware and software have considerably short life cycles. In the business community, workstations, servers, networking equipment, and mobile devices are replaced regularly. Technology upgrades are driven by rapidly increasing business application performance demands. Security requirements also drive technology upgrades. With the exponentially increasing incidents of data breaches, corporate espionage, and other cybercrimes, the business community must have the latest technological advances to protect their critical assets from sophisticated attacks.

Because the business world replaces older technology at such a rapid pace, as hardware and software reach the end of their useful life in the marketplace, the manufacturer will designate the product as "End-of-life" (EOL). When hardware has reached EOL, the manufacturer will discontinue support, services, and the availability of spare parts. With software and operating systems, the vendor will discontinue telephone and email support, the release of bug fixes, and security updates when designated EOL.

However, in the gaming industry the applications are developed for a specific hardware platform, such as a slot machine, which is static and does not change. Gaming applications do not continuously demand greater performance from the hardware. As a result, the gaming industry has not been required to continuously refresh outdated hardware and operating systems. The systems remain stable, functional and profitable for many years, but without as much pressure to continuously update as is present in other industries the hidden dangers of outdated and unsupported technology have been ignored.

The NIGC has recognized the security risks associated with outdated Class II gaming systems and has attempted to impose regulatory security controls. Yielding to pressures from the gaming industry, the NIGC has allowed these highly vulnerable systems to be grandfathered for 10 years. On November 10, 2018, these grandfathered systems must be made compliant with regulatory controls or be removed from the gaming floor. Some in the industry believe the grandfather waiver should be extended even longer for these obsolete and vulnerable systems.

The bottom line is that allowing the outdated technology used in these grandfathered systems to continue to be used is putting the gaming industry at considerable risk of serious cyber-attacks that may lead to a breach of customer trust, financial losses, and data compromise. Furthermore, the vulnerabilities inherent in the grandfathered systems also put newer and compliant systems at risk of compromise.

Security and Outdated Technology

Security risks are the number one danger of older technology. The older the operating system, the longer the hackers have had to find and exploit vulnerabilities. This is especially true when the manufacturer has designated the operating system to be EOL and is no longer actively maintaining support. If the firmware is old and outdated, the risk of a major security incident doubles.

Obsolete systems are exposed to countless and constantly increasing security vulnerabilities. In fact, research shows that over 10,000 new malware threats are discovered each hour. With outdated technology, the risk is constantly increasing at exponential rates.

Older Operating System Risks

Microsoft's Windows XP operating system is designated EOL and unsupported. This is the most common operating system found in the grandfathered Class II gaming systems manufactured before November 10, 2008.

A system running Windows XP is 6x more likely to be infected with malware than a system running Windows 10.

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information security vulnerabilities and exposures. The National Cybersecurity Federally Funded Research and Development Center, operated by the MITRE Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security.

According to the CVE, Windows XP has 729 known vulnerabilities. 129 of these vulnerabilities have been patched by Microsoft when it was still a supported operating system. There are 22 known exploits of Windows XP vulnerabilities. Since Windows XP is EOL and unsupported, 600 known vulnerabilities remain unpatched and exposed to immediate attacks. Even this grim outlook is optimistic, as it assumes that all of the 129 Microsoft patches have been applied. With the grandfathered Class II gaming systems, it is highly unlikely these patches have been installed. Patched or unpatched, Windows XP systems are an easy target for cybercriminals.

2017 has been an especially bad year for the security of Windows XP and other EOL Microsoft operating systems. The National Security Agency (NSA) had developed a classified toolkit that was only known to the agency and used by the agency to exploit Windows vulnerabilities. This toolkit was stolen from the NSA by an underground group of cybercriminals known as Shadow Brokers and released to the public.

While Microsoft reluctantly released an “emergency patch” for unsupported operating systems, it only addressed some of the vulnerabilities that can be exploited by the NSA Toolkit.

The other common Operating System in use by grandfathered games is Linux. The Linux OS available in 2008, of which there were ten varieties, were all designated EOL before 2013. Linux being a free OS also means that it is supported only by the community and does not have official personnel protecting its security. Users come up with answers for security holes and then they release a new distribution. This also means that there are some security issues that are never addressed due to the time constraints faced by volunteer efforts.

Considering that grandfathered Class II gaming systems are unpatched, the threats posed by the NSA Toolkit, other known exploits, and unknown exploits is an indisputable argument for removing grandfathered systems from gaming floors.

Outdated Firmware Vulnerabilities

Firmware is software written to a rewritable chip, such as the BIOS chip, a hard drive controller chip, and so on. Almost every electronic device has a rewritable firmware chip.

Computers rely on fundamental system firmware, commonly known as the system Basic Input/output System (BIOS), to facilitate the hardware initialization process and transition control to the operating system. The BIOS is typically developed by the original equipment manufacturers (OEMs) and independent BIOS vendors and is distributed to end-users by motherboard or computer manufacturers.

Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS’s unique and privileged position within the PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on a system—either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

Firmware attacks recur on a regular basis. To combat them, BIOS manufacturers have created more defensible firmware versions, and in 2011, the National Institute of Standards and Technology (NIST) published two firmware protection guidance documents: Special Publication 800-147 (PDF) and Special Publication 800-155 (PDF).

The gold standard of firmware protection is defined in the NIST documents and has culminated in the open BIOS specification called UEFI (Universal Extensible Firmware Interface), considered the first strongly secure boot firmware standard. It requires trusted roots, digital certificates, and digital signatures.

Unfortunately for older systems, UEFI 2 requires different chipsets than pre-UEFI motherboards. Microsoft's Windows Secure Boot technology only began offering UEFI protections with Windows 8- and 2012-certified computers. As a result, grandfathered systems are more vulnerable to firmware attacks that would likely include malware, surveillance, theft.

Outdated Hardware Risks

Old hardware has vulnerabilities that cyber-criminals can take advantage of to breach systems. The longer hardware has been available to the public, the longer criminals have had to find their cyber and physical weaknesses.

Because of this, just as with software manufacturers, hardware manufacturers assume customers will upgrade their assets to cover the latest issues, most of which include enhanced functionality, greater performance and security.

With outdated hardware, the greatest risk is the absence of security features. When hardware is considered obsolete (EOL), most organizations will upgrade the hardware or deploy compensating controls to protect against threats to the system. In the Class II gaming industry, the NIGC's Minimum Technical Standards serve as the compensating controls. This is why it is so important that these controls be implemented across all Class II gaming machines.

The hardware used in the grandfathered gaming systems have been known to the public for 10 years and these systems are exempt from many of the compensating controls offered by the Minimum Technical Standards. As a result, these systems pose a clear risk to the gaming industry.

Risks to Compliant Systems and Gaming Infrastructures

According to BitSight Security Ratings, if half of a network's endpoints are outdated, the chances of the entire network experiencing a breach nearly triples. These findings underscore the seriousness of the risk posed by outdated software, operating systems, firmware, and hardware.

As we have established the risk associated with grandfathered systems, it should be noted that these outdated systems also pose a serious threat to compliant systems and the gaming infrastructures as a whole. Grandfathered systems can be easily compromised and used as a pivot point for attacking or compromising other systems on the same internal networks. If even one manufacturer has grandfathered games on a casino floor, every other game on the network, compliant or not, is at risk. This may put casinos in a difficult liability situation given

that they have allowed fully compliant machines owned by others to be put at risk under their supervision by allowing vulnerable machines into the same network.

Casino and Gaming Firm Incidents

Given the volume of financial data and the likelihood of gaming fraud, casinos and gaming firms are an ideal target for cyber-attacks.

Theoretically, gaming floors operate on closed networks. However, there are documented incidents where closed casino networks have been connected to public networks. An example of this is the casino that was compromised due to an internet connected fish tank. With the increased usage of mobile devices, wireless networking technologies, and internet connected devices, the risk of cyber criminals infiltrating gaming floor networks and compromising the extremely vulnerable grandfathered Class II gaming systems is continuously increasing.

CONCLUSION

According to the SANS Institute 2017 Threat Landscape Survey, Endpoint devices (an Internet-capable computer on a TCP/IP network) are on the front lines of the cybersecurity battle. They represent the most significant entry points for attackers obtaining a toehold into the network.

Systems that have not been updated since November 10, 2008 are technologically obsolete and are at higher risk of compromise. As discussed in this report, the vulnerabilities introduced by outdated and unpatched software, operating systems, firmware and hardware provide the perfect target for cybercriminals. These systems are also an entry point that can be used to launch more sophisticated attacks on regulatory compliant systems. By attacking and compromising the highly vulnerable grandfathered system, the cybercriminal can pivot and use these systems to compromise other compliant systems and casino's infrastructure, including point-of-sale (POS) systems, accounting systems, voucher systems, communication devices, network security safeguards, and physical security controls.

This method of pivoting from the soft targets (systems that are easily compromised) to compromise every computer and device on the network is the primary tactic used by sophisticated attackers.

Casinos and the gaming manufacturers are a target for cybercriminals and this industry must improve its cyber security capabilities. The NIGC intent to require obsolete systems

manufactured before November 10, 2008 to comply with the Minimum Technical Standards will significantly improve the cybersecurity of casinos and gaming floor systems.

Appendix A of this report provides an analysis of the Minimal Technical Standards provided in 25 CFR 547. The conclusion of this analysis is that the absence of these controls in grandfathered systems significantly increase the risks to the integrity, confidentiality, accountability, and fairness of play for Class II gaming systems.

See attachment for Appendix A.

APPENDIX B: REFERENCES

NIST Information Security Handbook, Special Publication 800-100 (October 2006)

<https://csrc.nist.gov/publications/detail/sp/800-100/final>

NIST BIOS Protection Guidelines, Special Publication 800-147 (April 2011)

<https://csrc.nist.gov/publications/detail/sp/800-147/final>

NIST BIOS Integrity Measurement Guidelines Special Publication 800-155 (December 2011)

https://csrc.nist.gov/CSRC/media/Publications/sp/800-155/draft/documents/draft-SP800-155_Dec2011.pdf

SANS - Information Security Resources | Information Security Policy

<https://www.sans.org/security-resources/policies>

Center for Internet Security CIS Critical Security Controls

<https://www.cisecurity.org/>

The Importance of Cyber Hygiene in Cyberspace

<http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace>

U.S. Casinos, Regulators Face Growing Cybersecurity Challenge

https://gamblingcompliance.com/premium-content/news_analysis/us-casinos-regulators-face-growing-cybersecurity-challenge

Verizon 2017 Data Breach Investigations Report

<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

Data Security Breach Articles:

articles that have data and statistics on cybersecurity

<http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/>

<https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>

https://en.wikipedia.org/wiki/List_of_data_breaches

https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

<https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Timeline.pdf>

<https://gcn.com/articles/2013/05/30/gcn30-timeline-cybersecurity.aspx>

https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Significant_Cyber_Events_List.pdf?Sm9UDh1TitdFtv3BIXO3tkIHRVfanwdE

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf

<https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23>

<https://www.securable.io/infosec-news/infosec-update-cyber-security-education-hacking-more-than-just-computers>

<https://www.upguard.com/blog/casino-data-breaches-and-doubling-down-on-digital-resilience>

<https://www.csoonline.com/article/3089449/security/hard-rock-las-vegas-suffers-a-second-data-breach.html>

<http://www.zdnet.com/article/hard-rock-loews-hotels-admit-data-breach/>

<https://www.securelink.com/securelink-blog/is-your-casino-network-under-attack/>

<https://www.bankinfosecurity.com/casino-sues-trustwave-over-data-breach-a-8804>

<https://globalnews.ca/news/3208546/security-experts-call-grey-eagle-casino-security-breach-a-wake-up-call/>

<https://www.darktrace.com/resources/wp-global-threat-report-2017.pdf>

<https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Gus-Frischie-and-Evan-Teitelman-Backdooring-the-Lottery.pdf>

The Need for Minimum Technical Standards for Class II Gaming Systems in the Context of Cyber Vulnerabilities – A Modern Day Imperative

Submitted by:

Sage Policy Group, Inc.

Submitted to:

Coalition for Fair Gaming, LLC

November 2017

Table of Contents

Executive Summary.....	3
Introduction.....	4
I. Incorrect Rationale for Exemptions	4
II. Growing Security Threats	9
III. Propitious Timing.....	10
Conclusion	12
Sage Policy Group, Inc.	13

List of Exhibits

Exhibit 1: Gaming machines growth ranked by state, 2008-2015.....	5
Exhibit 2: Gaming revenue growth ranked by state, 2014-2015.....	6
Exhibit 3: Class II Machines in states operating only Class II machines, 2006-2015.....	7
Exhibit 4: Indian Gaming Revenues, 2000-2015	10
Exhibit 5: Nominal Gross Gaming Revenue, FY07-FY16	11

The Need for Minimum Technical Standards for Class II Gaming Systems in the Context of Cyber Vulnerabilities – A Modern Day Imperative

Executive Summary

In 2008, the National Indian Gaming Commission (NIGC) promulgated Minimum Technical Standards for Class II Indian gaming (“Minimum Technical Standards” or “Standards”). These Standards were passed in an effort to “address and mitigate activity that jeopardizes the integrity of Indian gaming” and “swiftly act on anything that jeopardizes the health and safety of the public.”¹

In response to concerns regarding these Standards, the NIGC commissioned a study (the “Meister Report”) which concluded that the Standards would cause hardship by reducing gaming and non-gaming revenues, resulting in the closure of certain gaming facilities and decreasing the number of tribal member jobs.² Relying on the Meister Report, the NIGC deployed a “Grandfather period,” which delayed the date by which older Class II games were required to comply with the Minimum Technical Standards — first until 2013, and subsequently until 2018.

History indicates that there was no basis for concerns that these contemporary standards would negatively impact tribes. The experience of the last decade, during which implementation of these new standards was required for all newly-built Class II games, has shown that the Meister report was erroneous. Compliant Class II games are thriving. Data characterizing the past decade indicate that meeting new requirements has been both feasible and necessary given the rapidly spreading specter of cyber-criminality threatening both the integrity of Indian gaming and public safety.

This report concludes that the NIGC’s proposed rule to permanently exempt older machines from the vast majority of the Minimum Technical Standards will generate a host of negative outcomes for tribal stakeholders. While the benefits sought by grandfathering proved illusory, the risks are expanding. Security concerns intensify as grandfathered machines fall further behind the technical curve. Risks of a major security breach asymptote to virtual certainty, with many hidden costs accompanying these risks.

¹ National Indian Gaming Commission, *Our Mission*. <https://www.nigc.gov/commission/principles-and-priorities>. Accessed October 16, 2017.

² Meister, Alan. 2008. *The Potential Economic Impact of the October 2007 Proposed Class II Gaming Regulations*. Commissioned by the National Indian Gaming Commission. February 1, 2008. Page 3.

Introduction

The National Indian Gaming Commission (NIGC) implemented a five-year grandfather period, followed by a second five-year period, during which existing Class II gaming systems were exempted from the Minimum Technical Standards found in 25 C.F.R. 547.³ The purpose of the grandfather periods was to negate any negative economic consequences of mandating immediate compliance and to allow Indian gaming facilities time to bring their machines into compliance. This second five-year grandfather period is set to expire on November 10th, 2018.

This report: 1) analyzes the predictions that served to justify the two prior grandfather periods, concluding that the predictions were faulty and have proven incorrect; 2) discusses the growing threats of non-compliance; and 3) examines the current state of Class II gaming and the broader economy.

I. Incorrect Rationale for Exemptions

A 2008 report titled “The Potential Economic Impact of the October 2007 Proposed Class II Gaming Regulations” (The Meister report)⁴ set forth a number of arguments against implementing Minimum Technical Standards on Class II gaming machines.

The Meister report argued that because compliant Class II machines would be slower, more cumbersome to play, confusing, and less diverse, they “would be less appealing to patrons and generate less gaming revenue than existing Class II machines.”⁵ This argument was predicated on the assumption that the compliant Class II Electronic Gaming Machines (EGMs) would require a player to press a button at least two times in order to buy a bingo card, mark their bingo card, and claim their prize.⁶ As a result, individual games would take longer and patrons would play fewer games per hour at a compliant Class II EGM. While at the time compliance standards that required at least two button presses to win were, indeed, under consideration,⁷ they were never implemented.

The incorrect assumption that Class II EGMs would be slower is critical to Meister’s analysis. The Meister report presented three different scenarios to estimate lost gaming revenue as a result of

³ 25 CFR Part 547 - MINIMUM TECHNICAL STANDARDS FOR CLASS II GAMING SYSTEMS AND EQUIPMENT

⁴ Meister, Alan. 2008. *The Potential Economic Impact of the October 2007 Proposed Class II Gaming Regulations*. Commissioned by the National Indian Gaming Commission. February 1, 2008.

⁵ The Meister Report, page 14

⁶ *Id.*

⁷ The Meister Report, pages 9-14.

fewer machines and diminished revenue per machine due to compliance,⁸ ranging from more than \$1.2 billion to \$3.7 billion.⁹

Existing data regarding the growth of activity in compliant Class II gaming, both in terms of quantity of machines and associated revenue, indicate that these machines have been at least as attractive to players as non-compliant machines. If Meister's predictions were accurate, new compliant machines would have under-performed compared to legacy equipment, which would have induced slower machine replacement rates as casinos strove to hang on to their older, non-compliant machines for as long as possible. This effect would have been even more pronounced in facilities operating only Class II machines, which could not add growth through Class III machines to compensate for the predicted problems with new Class II games. Instead, the available data shows the opposite.

Exhibit 1: Gaming machines growth ranked by state, 2008-2015

Rank	State	2008-2015 CAGR	Rank	State	2008-2015 CAGR
1	Alabama	11.9%	15	New Mexico	1.0%
2	Texas	10.2%	16	California	0.6%
3	Nebraska	6.9%	17	Colorado	0.6%
4	Montana	4.3%	18	Oregon	0.5%
5	North Carolina	4.0%	19	Minnesota	-0.2%
6	Oklahoma	3.8%	20	New York	-0.3%
7	Florida	3.2%	21	Louisiana	-0.7%
8	South Dakota	2.9%	22	Wisconsin	-0.8%
8	Wyoming	2.9%	23	Iowa	-0.9%
10	Washington	2.0%	24	Idaho	-1.0%
11	Arizona	1.9%	25	Nevada	-1.3%
12	Michigan	1.8%	26	Kansas	-1.7%
13	North Dakota	1.6%	27	Mississippi	-3.3%
14	Alaska	1.5%	28	Connecticut	-5.2%

Source: Casino City's Indian Gaming Industry Report, 2017 Edition

Exhibit 1 above is particularly revealing. It shows that instead of the slowest growth rates, three of the four states that exclusively utilized Class II machines (Alabama, Texas, and Nebraska) experienced the *fastest* growth in machine population between 2008 and 2015. The stock of machines in Alabama and Texas increased by more than 10 percent per annum over this period.

Even narrowing the analysis to include only states with Indian gaming facilities, those states that could only grow with compliant Class II games still outperformed their counterparts. From 2014 to

⁸ The Meister Report, page 45.

⁹ In 2013 dollars to reflect the loss at the end of the first grandfather period.

2015, Indian gaming facilities in Texas experienced faster gaming revenue growth (15.5 percent) than any of the other twenty-seven states. Alabama ranked second with 11.1 percent year-over-year revenue expansion. This is overwhelming evidence proving the popularity of compliant Class II machines. They are much more than simply viable or acceptable, they are thriving in the marketplace. Exhibit 2 supplies relevant statistical detail.

Exhibit 2: Gaming revenue growth ranked by state, 2014-2015

Rank	State	2015 Growth %	Rank	State	2015 Growth %
1	Texas	15.5%	15	Wisconsin	3.5%
2	Alabama	11.1%	16	Minnesota	3.5%
3	North Carolina	10.9%	17	Oregon	3.0%
4	South Dakota	10.8%	18	New Mexico	2.8%
5	Florida	9.3%	19	Kansas	2.5%
6	California	8.0%	20	Colorado	2.4%
7	Idaho	7.4%	21	Michigan	1.7%
8	Oklahoma	6.7%	22	North Dakota	1.4%
9	Montana	6.3%	23	Iowa	0.9%
10	Mississippi	5.0%	24	Louisiana	0.3%
11	Arizona	5.0%	25	New York	-0.4%
12	Washington	4.6%	26	Connecticut	-1.2%
13	Nebraska	4.5%	27	Nevada	-4.3%
14	Alaska	4.2%	28	Wyoming	-14.4%

Source: Casino City's Indian Gaming Industry Report, 2017 Edition

Narrowing the analysis further to the tribes that only operate only Class II games yields similar repudiations of Meister's predictions. Alabama, Alaska, Nebraska, and Texas operate only Class II machines within their gaming facilities.¹⁰ 2007 was the final full year during which non-compliant machines could be procured. That year, only 11 new machines were placed in those four states representing growth of approximately 0.3 percent. If Meister's report were correct, one would expect to see that meager growth rate spike in early 2008 as casinos bought up as many non-compliant machines as they could before regulations went into effect. After that year, machine placement would presumably dwindle.

In fact, growth did surge in 2008, by 22.1 percent. However, instead of falling off as anticipated, growth continued thereafter driven purely by compliant Class II machines. The year 2009 was associated with 11.9 percent growth, which was followed by 2010's 9.8 percent performance. In

¹⁰ Meister, Alan. 2017. *Casino City's Indian Gaming Industry Report, 2017 Edition*. Page 33.

2012, growth totaled 16.9 percent. Growth has continued since, often by double-digits on a per annum basis. (Exhibit 3)

Perhaps the most telling example is Alabama, where Meister's dire predictions pointed to diminished revenue, shuttered facilities, and foregone tribal employment. Rather than experiencing a collapsing marketplace, Alabama witnessed its Class II machines increase by 142 percent from 2,600 in 2008 to 6,300 just five years later. As indicated above, Alabama had the second highest revenue growth of all states in 2015.

Based on these data and insights, the introduction of compliant Class II machines has had no discernible negative impact on the marketplace. The market for Class II gaming continued to be vigorous in areas adding compliant machines even during a period punctuated by the Great Recession. Facilities in these four states (Texas, Alabama, Nebraska, Alaska - Exhibit 3) added nearly 5,900 compliant machines between 2008 and 2015. Compliant machines collectively represent a majority of machines now in operation in these four states.

Exhibit 3: Class II Machines in states operating only Class II machines, 2006-2015

	2006	2007	2008 ¹¹	2009	2010	2011	2012	2013	2014	2015	CAGR ¹²
Alabama	2,101	2,052	2,600	3,000	3,270	4,200	4,769	6,300	6,337	6,400	11.8%
Alaska	30	40	80	80	80	90	90	80	90	90	11.6%
Nebraska	314	318	389	449	478	483	490	651	666	662	7.7%
Texas	1,325	1,371	1,548	1,638	1,844	1,858	1,988	2,786	2,796	3,357	9.7%
Total	3,770	3,781	4,617	5,167	5,672	6,631	7,337	9,817	9,889	10,509	10.8%

Source: Casino City's Indian Gaming Industry Report, 2017 Edition

One could argue that Class II machine growth in these four states is attributable to a lack of competition from Class III machines, which aren't permitted there. However, even the Meister Report agrees that competition for gaming dollars has been on the rise even where Class III facilities are prohibited because of the emergence of alternative forms of gambling.

For example, the Meister Report explains in detail the rising competition encountered by Alabama's Indian gaming facilities. In 2003, greyhound racetracks began operating electronic bingo machines that are faster than those operated at Indian gaming facilities. Three years later, Alabama began operating "sweepstakes machines," which emulate the look and feel of slot machines.¹³ Despite

¹¹ This is the year in which the technical standards were implemented. Despite the grandfather period, all subsequently manufactured Class II machines had to comply with the standards after this point.

¹² For ten-year period from 2006 to 2015.

¹³ The Meister Report, pages 26-27

increasingly intense competition, Alabama's Class II EGMs have become increasingly popular and accessible to consumers.

Another argument against the faithful implementation of Minimum Technical Standards was that Indian gaming facilities would incur large, upfront capital costs. The Meister report predicted capital, deployment, and compliance costs in the range of \$267.2 million to \$654.3 million.¹⁴ Even though such costs would apply to manufacturers, not Indian gaming facilities, Meister's report asserted that "these are good estimates of the increased costs to tribes assuming that such costs are passed through to tribes."¹⁵ That assertion is both highly speculative and misplaced. All Class II EGM manufacturers that have placed new games since 2008 have now been building compliant systems for years. Moreover, the Indian gaming market relies heavily, often exclusively, on leased machines as opposed to purchased machines. Because vendors are willing to supply compliant Class II EGMs that perform at least as well as their non-compliant predecessors, there are facially no economic burdens to tribes that are required to replace non-compliant machines as leases expire.

The Meister Report also estimates lost non-gaming revenue as a result of the October 2007 proposed regulations.¹⁶ The notion was that fewer players on compliant machines would translate into diminished visitation and less consumer spending on non-gaming activities and items. His analysis is a simple one and applies the ratio of Class II machine-related non-gaming revenue to Class II machine revenue. The resulting estimated lost non-gaming revenue ranges from \$25.6 million to \$79.4 million.¹⁷ But this estimate of lost non-gaming revenue is based upon yet another layer of speculation that all his earlier suppositions were true. Available evidence suggests that these earlier presumptions and predictions were invalid. Correspondingly, Meister's estimates of lost non-gaming revenue have proven inaccurate.

The Meister Report states that "previous research has shown that there is a strong correlation between gaming revenue and number of gaming-related employees." Based on his assumption that compliant Class II games must be slower, less profitable, and less patronized, he claims that tribal member jobs would be lost as a result.¹⁸ However, since gaming revenues have tended to rise with the growing prevalence of compliant Class II EGMs, it seems clear that the introduction of compliant EGMs has not reduced employment opportunities for tribal members.

¹⁴ The Meister Report, page 56.

¹⁵ *Id.* at 57

¹⁶ *Id.* at 51

¹⁷ *Id.* at 52

¹⁸ *Id.* at 59

II. Growing Security Threats

Not only are the economic factors pointing towards requiring compliance, there are rapidly expanding security concerns related to increasingly vulnerable non-compliant EGMs. Specifically, the existence of non-compliant Class II machines renders Indian gaming facilities susceptible to large-scale losses that could outweigh any remaining costs associated with bringing pre-2008 Class II machines into compliance.

This notion that a casino could fall victim to digital fraud is hardly conjecture. In 2014, a group of Russian scammers exploited a defect in slot machines and were able to steal more than \$10,000 a day from a single casino.¹⁹ There exists a Russian business with a singular focus upon the use of algorithms to reverse engineer the timing of EGMs. This business sends operatives to targeted casinos around the world to exploit vulnerabilities.²⁰ Most of these exploits are targeted at older machines, for example Aristocrat's Mark VI model machine,²¹ specifically because they lack the protections of modern machines.

According to a report by Darktrace, a cybersecurity firm that monitors digital vulnerabilities, hackers have also breached a North American Casino's internal data through an internet-connected fish tank, stealing more than 10 GB of potentially sensitive data in the process.²² Continuing to allow Indian-operated gaming facilities to be vulnerable to such attacks is at odds with sensible public policy.

One need not look exclusively to the gaming industry for evidence of vulnerability. Equifax, a consumer credit reporting agency with technical resources far in excess of any individual gaming facility, recently fell victim to a hack that exposed the sensitive personal information of more than 143 million Americans.²³ Equifax's market capitalization plunged from \$17 billion to \$11.2 billion during the week that followed. Within two weeks of the Equifax hack becoming public, the U.S. Securities and Exchange Commission announced that one of its filing systems had been breached.²⁴

Based on available evidence and recent history, we conclude that a single technical breach could cost a gaming facility millions of dollars. This represents the most important reason to disallow

¹⁹ Koerner, Brendan. Wired. *Russians Engineer a Brilliant Slot Machine Cheat—and Casinos have no Fix*. February 6, 2017.

²⁰ Koerner, Brandon. Wired. *Meet Alex, the Russian Casino Hacker Who Makes Millions Targeting Slot Machines*. August 5, 2017.

²¹ Koerner, Brendan. Wired. *Russians Engineer a Brilliant Slot Machine Cheat—and Casinos have no Fix*. February 6, 2017.

²² Schiffer, Alex. The Washington Post. *How a fish tank helped hack a casino*. July 21, 2017.

²³ Gressin, Seena. The Federal Trade Commission. *The Equifax Data Breach: What to do*. September 8, 2017.

²⁴ Lynch, Sarah. Reuters. *Hack of Wall Street Regulator Rattles Investors, Lawmakers*. September 21, 2017.

permanent grandfathering of non-compliant machines. The older, non-compliant Class II machines represent massive sources of potential loss and liability to Indian gaming facilities. Non-compliant machines rely upon software and operating systems that are at least nine years old, that have been publicly accessible for several years, and that do not meet contemporary Minimum Technical Standards.

III. Propitious Timing

Economic uncertainty in the wake of the Great Recession represented a primary motivator for the second grandfather period that began in 2013. Gaming revenues had stagnated over the prior five years (see Exhibit 4) and there was a natural reluctance to layer additional costs on Indian gaming facilities.

Exhibit 4: Indian Gaming Revenues, 2000-2015

	Actual \$ (millions)	Nominal Growth	2015 \$ (millions)	Real Growth
2000	\$10,958.7	11.8%	\$15,083.6	8.2%
2001	\$13,137.8	19.9%	\$17,582.6	16.6%
2002	\$15,122.7	15.1%	\$19,924.0	13.3%
2003	\$17,366.5	14.8%	\$22,370.4	12.3%
2004	\$20,039.2	15.4%	\$25,143.6	12.4%
2005	\$22,888.2	14.2%	\$27,771.1	10.4%
2006	\$25,219.0	10.2%	\$29,649.5	6.8%
2007	\$26,352.6	4.5%	\$30,124.3	1.6%
2008	\$26,782.2	1.6%	\$29,483.7	-2.1%
2009	\$26,485.6	-1.1%	\$29,260.9	-0.8%
2010	\$26,741.9	1.0%	\$29,067.2	-0.7%
2011	\$27,618.4	3.3%	\$29,101.3	0.1%
2012	\$28,153.8	1.9%	\$29,064.0	-0.1%
2013	\$28,315.2	0.6%	\$28,808.6	-0.9%
2014	\$28,906.9	2.1%	\$28,941.2	0.5%
2015	\$30,491.7	5.5%	\$30,491.7	5.4%

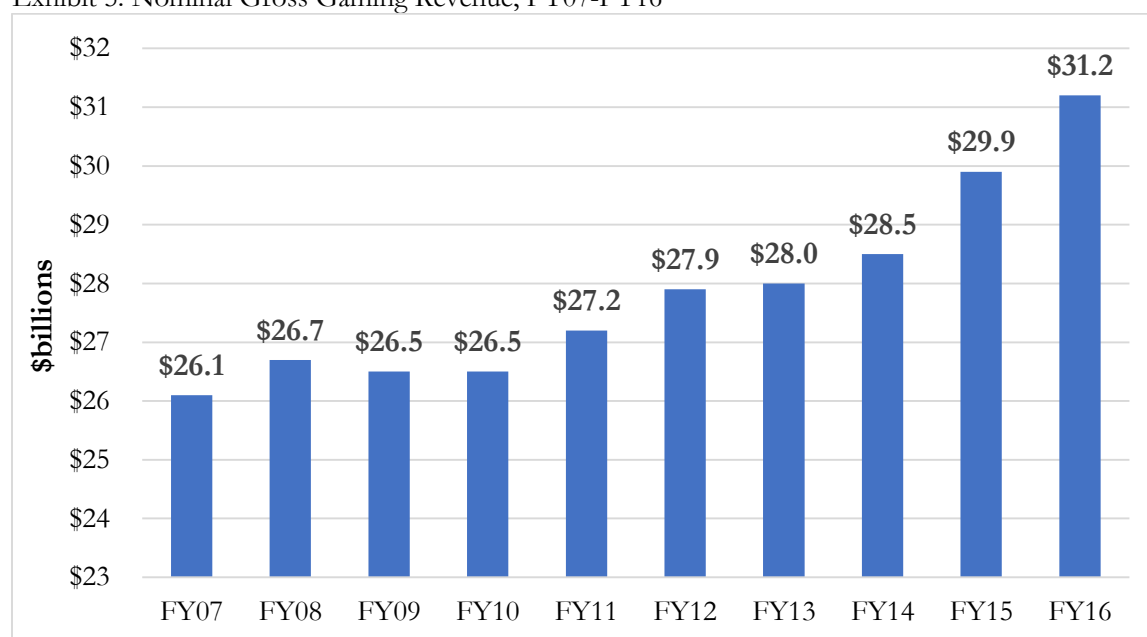
Source: Casino City's Indian Gaming Industry Report, 2017 Edition

As of this writing, the U.S. is in its ninth year of economic recovery. This is now the third lengthiest expansion cycle in American history. Gross domestic product has increased in twenty-four of the previous twenty-five quarters. As of this writing, unemployment is at roughly a 17-year low and

national employment has increased for eighty-five consecutive months, the longest streak on record.²⁵

A recent Federal Reserve report indicates that net household wealth has never been higher in America.²⁶ Wealth gains are attributable to both a surging stock market and ongoing gains in housing values. Consumer spending growth continues to push the broader U.S. economy forward, helping to explain the economic outperformance of areas such as Las Vegas and Orlando. The nation also boasts a record number of job openings (6.2 million), rising median household incomes, and declining poverty rates.²⁷

Exhibit 5: Nominal Gross Gaming Revenue, FY07-FY16



Source: NIGC

Predictably, broader economic strength has translated into improving gaming revenues. According to the NIGC, gross gaming revenues surpassed \$30 billion for the first time in FY2016, jumping to \$31.2 billion. Revenues expanded 9.5 percent from FY2014 to FY2016 after expanding just 4.9 percent during the prior six-year period. Despite the Great Recession, revenues doubled during the 2000-2015 period.

²⁵ U.S. Department of Labor, Bureau of Labor Statistics. *The Employment Situation—August 2017*. September 1, 2017.

²⁶ Board of Governors of the Federal Reserve System. *Report on the Economic Well-Being of U.S. Households in 2016*. May 2017.

²⁷ U.S. Department of Commerce, Bureau of Economic Analysis. *Gross Domestic Product: Second Quarter 2017 (Second Estimate)*. August 30, 2017.

A September 2017 press release from the Federal Reserve’s Open Market Committee predicts that over the next few years “economic activity will expand at a moderate pace, and labor market conditions will strengthen somewhat further.”²⁸ As indicated by Exhibit 5, nominal gross gaming revenue has been racing higher since FY2014. In short, this represents a propitious moment to invest in the future of Indian gaming by replacing vulnerable, non-compliant machines with modern, safer ones.

Conclusion

This report concludes that:

1. The introduction of compliant Class II machines has not negatively impacted Indian gaming facility revenues. In fact, revenue growth has been far sharper in contexts in which these machines have been introduced.
2. Non-compliant machines still in operation at Indian gaming facilities represent a source of enormous digital vulnerability and fraud.
3. The current period represents an advantageous economic environment in which to replace non-compliant machines with compliant ones.

As indicated in this report, many of the capital costs associated with transitioning from non-compliant to compliant Class II machines have already been incurred over the decade-long grandfathering period. It makes sense to complete the transition, reducing cyber-vulnerability and associated financial risks facing Indian gaming facilities in the process. A permanent grandfathering of non-compliant Class II EGMs is therefore not justified on the basis of sound public policy.

²⁸ Board of Governors of the Federal Reserve System. *Federal Reserve issues FOMC statement*. September 20, 2017.

Sage Policy Group, Inc.

Sage Policy Group, Inc., a Sub Chapter S Corporation, was established in 2004 by Anirban Basu. Sage is an eleven-person economic and policy consulting firm specializing in economic, fiscal and legislative analysis, program evaluation, and organizational and strategic development. The firm's clients include public agencies at every level of government, law firms, developers, money managers, and an array of nonprofit organizations operating in a variety of segments. As experts in research methods, our corporate focus is to utilize sound, widely accepted analytical techniques that provide our clients and their stakeholders with valid and reliable knowledge and information to support critical organization and decision-making requirements.

Over the course of its 13-year history, Sage has conducted many studies related to gaming. Gaming-related clients include The Maryland Jockey Club, the Horseshoe Casino in Baltimore, casino developers in Delaware, the Maryland Horse Breeders Association, and the developers of a new \$1.2 billion casino at National Harbor in the Washington metropolitan area.

Russian Slot Cheating Team

A Reference Guide

July 15, 2014
Authored by: Darrin Hoke

Russian Slot Cheating Team

A Reference Guide

Origins

From February 2011 through November 2012 there were several reports out of Europe and Eastern Europe that Novomatic Slot Machines (Austrian based company) were possibly being cheated by a group of individuals mostly made up of Russian and German Nationals? These reports remained unconfirmed and Novomatic released a number of Customer Notifications in 2011.

In addition to the Novomatic games there were reports that Atronic games (Germany based company) and Mega Jack games (Russian based company) were also being cheated. Most of the reports indicated that the suspects were filming the game play of these machines with a cellphone and then coming back a short time later and taking advantage of the game. Some of the reports suggested that the individuals involved possibly had inside information from the manufacturer regarding a vulnerability in the operating system. In any event, none of the reports were conclusive as to a method of cheating or the presence of a cheating device. In addition, most of the suspects were not arrested and any arrests that did occur did not include any details.

There are as many as 25 individuals identified as participating in these cheating events and another 7 who have not been identified. Names, identifying information, and photographs are attached at the end of this report (if available).

United States May – June 2014

On June 9th 2014 a St. Louis, MO casino put on an alert regarding some suspicious slot play on Aristocrat Mark VI platform games. Slot forensics showed the machine was producing a significant win for the suspect with nominal coin in amounts. In this case the subject was inserting \$20 - \$60 at each game and cashing out vouchers valued at \$450 - \$1300. As additional properties began their follow-up it was discovered that there was a similar modus operandi at several properties across Missouri with each property reporting losses that \$9,000 - \$15,000 per visit by one or more of the suspects. Three suspects were identified as Murat Bliev, Mikhail Bahktin, and Sergei Smirnov as renting a car from Kansas City, MO airport and travelling to St. Louis, MO and turning in the rental car at the Chicago O'Hare airport.

A follow-up investigation indicated that three suspects are part of a larger group of Russian and German Nationals involved in cheating activities in Europe and Eastern Europe (see history). It was also discovered that many of these suspects travel to the US up to 8 times per year mostly coming into the country via the West Coast or East Coast. In addition it was discovered that one of the suspects was currently in the US and many of the suspects visited a large casino near Temecula, CA. On July 8th contact was made with this property and they were able to establish a number of prior visits dating back to September 2013 with the most recent visit as of June 21st 2014. The property was able to review video and observed the suspects using a device similar to a cellphone or PDA, which is consistent with the reports out of Missouri. They also noticed that cash out button the machines would flash very rapidly during odd times (not consistent with normal operations) and this mirrored a report out of Missouri where one property reported seeing the cash out button flash rapidly as the suspect approached the machine.

Russian Slot Cheating Team

A Reference Guide

Games Impacted

As of this writing only 1 game manufacturer has been identified as being vulnerable to this cheating event! Aristocrat Mark VI game platform with the following game themes;

- 50 Lions - 2002
- 100 Lions - 2006
- Geisha - 2001
- Heart of Gold - 2004
- Miss Kitty - 2006
- Pelican Pete - 2004
- Star Drifter - 2003

Most of these games are 50 lines/ 5 reel games with a credit buys 2 lines configuration (except 100 Lions/100 lines and Geisha 20 lines).

Game Forensics

These games have been forensically examined and at this time there is little evidence/information that can be obtained from the online slot system that would directly identify a cheating event occurred. There have been no reported variances in any of the BVA's and in many cases the BVA brands were different at the various properties. Financial examination of the impacted machines has been very consistent showing hold percentages by day being impacted at 50% - 400%. It is highly recommended that all properties research the identified game types for higher than normal hold percentage variances over the last 2 years.

Theories

The Aristocrat Mark VI platform is relatively older technology and there could be any number of methods being deployed to cheat these machines. The consistent use of a cellphone coupled with the fact that none of the suspects were observed manipulating the games directly by touching them is unusual and could indicate the use of a wireless technology. The SMIB (slot machine interface board), the UART (universal asynchronous receiver transmitter), the BVA (bill validator acceptor) and the BE2/AE2 (bonus engine) are all peripheral hardware devices that could be manipulated into artificially inflating the credit meter. The following picture shows a mock-up device that could be used to cheat electronic gaming devices/machines using the bonus engine.



Russian Slot Cheating Team

A Reference Guide

Update 07.15.2014

Mikhail Bahktin was arrested on July 14th 2014 at a Temecula, CA casino. Bahktin was in possession of 4 cellphones, one of which he was manipulating as he played an Aristocrat Mark VI platform game. The CA DOJ responded and took possession of the cellphones and Bahktin surrendered over \$6,000.00. Bahktin indicated that he and Sergei Smirnov were heading to Las Vegas, NV.

Russian Slot Cheating Team

A Reference Guide

Suspects

Subjects # 1,2,3

Photo #(s): 3

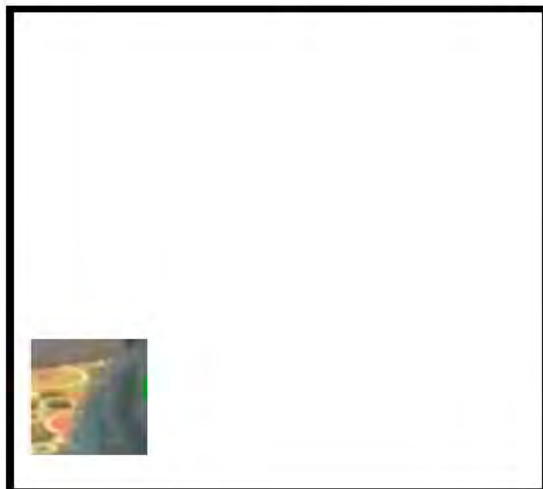
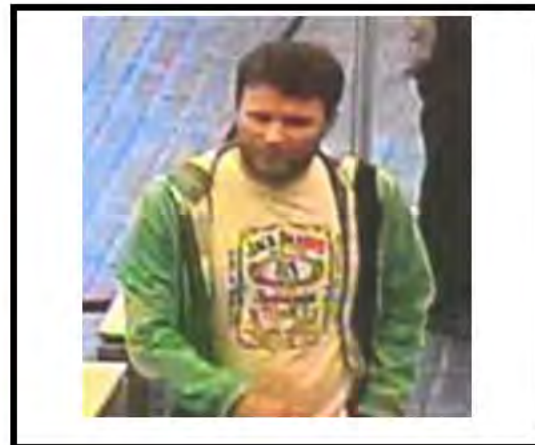
Photo Date: 6/1/2014

Photo Description(s):

Murat Bliev DOB
12.22.1977

Mikhail Bahktin DOB
07.08.1979

Sergei Smirnov DOB
08.01.1977

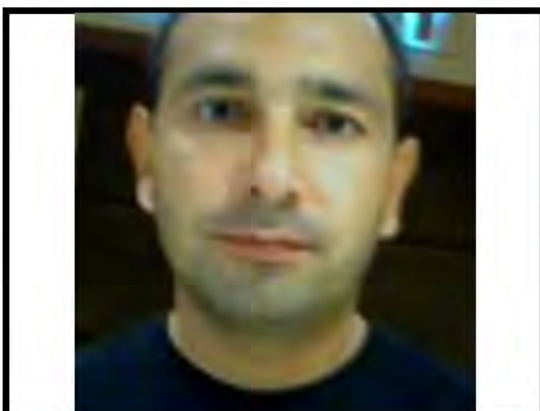


Russian Slot Cheating Team

A Reference Guide

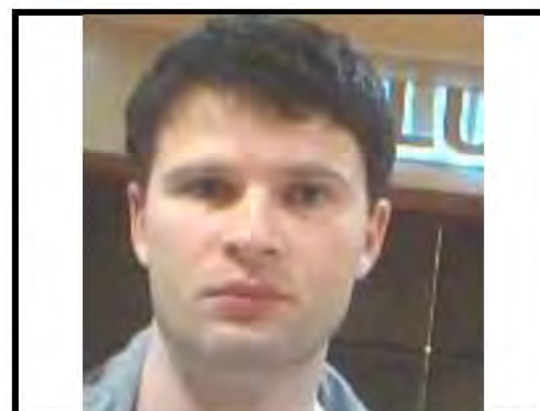
Subject # 1

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Murat Bliev Active in Missouri June 2014



Subject # 2

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Mikhail Bahktin Active in Missouri June 2014



Known Associate

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Alexander Belikov DOB 04/02.1972 Known Associate



Russian Slot Cheating Team

A Reference Guide

Known Associate

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Helga Eirich Poleschuk DOB 06.11.1978 Known Associate



Known Associate

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Thomas Eirich DOB 06/11/1976 Known Associate



Known Associate

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Igor Lavrenov DOB 05.21.1985 Known Associate Last Seen June 21 2014 in Temecula, CA



Russian Slot Cheating Team

A Reference Guide

Known Associate

Photo #(s): 2
Photo Date: Unk
Photo Description(s): Evgenii Logachev DOB 03.22.1982 Known Associate In the US as of July 2014



Additional Names

- Holger Jakubowski DOB: 04.18.1965 German National
- Christian Walczewski DOB: 12.19.1967 German National
- Anatoly Bala
 - Anatoly Associates
 - Felix Sayfytdinov Estonian
 - Alexander Aleshkin
 - Sergey Cherkasov
 - Vladislav Logachev
 - Alexander Belikov
 - Sergey Karpinsky
 - Vasylij Yuriev
- Alexey Maltsev DOB: 05.21.1968
- Tsilo Balabanov DOB: 03.01.1964 Bulgarian National
- Penko Radev DOB: 02.13.1970 Bulgarian National
- Dimitar Petkov DOB: 08.14.1971 Bulgarian National
- Oleg Cherepanov DOB: 01.30.1968
- Artem Alymov DOB: 10.25.1981

Comparison of price for Compliant and Non-compliant machines.

Description	Estimated Price		547.7 Regulation
	for Compliance	for non-Compliance	
Bill Validator	\$ 786.00	\$ 140.00	547.7 g
Printer	\$ 359.00	\$ 100.00	547.7 g
Sensors/Switches	\$ 22.00	\$ 22.00	547.7 g
Battery backup	\$ 65.00	\$ 65.00	547.7 All Regulations
Serial Number Plate	\$ 20.00	\$ 6.00	547.7 c,d
Touchscreen monitor	\$ 460.00	\$ 200.00	547.7 All Regulations
CPU	\$ 1,020.00	\$ 250.00	547.7 h,i
I/O Board	\$ 185.00	\$ 60.00	547.7 a,b,j
CPU connection	\$ 55.00	\$ 20.00	547.7 a,b
Reel Controller	\$ 120.00	\$ 80.00	547.7 a,b
Reels with Board	\$ 387.00	\$ 225.00	547.7 a,b
Storage Media	\$ 144.00	\$ 40.00	547.7 e
Dongles/Keys	\$ 27.00	\$ 25.00	547.7
Gaming Fee	\$ 300.00	\$ 300.00	547.7
Bells	\$ 36.97	\$ 17.00	547.7
UL FCC Testing (for parts required to be UL certified)	\$ 80.00	NA	547.7 h
SAS license	\$ 150.00	NA	547.7 g
COTS Class 3 Gaming Platform (amortized across EGMs)	\$ 300.00	NA	547.7 g
Total BOM Cost \$ 4,516.97 \$ 1,550.00			\$2,966.97

APPENDIX A: CONTROLS, RISKS AND EXPOSURE

- 1. Control 547.1: What is the purpose of this part?** The Indian Gaming Regulatory Act, 25 U.S.C. 2703(7)(A)(i), permits the use of electronic, computer, or other technologic aids in connection with the play of Class II games. This part establishes the minimum technical standards governing the use of such aids. **Risks Mitigated by Control:** Defining the “purpose” is essential for standards. Control 547.1 explains that these controls are intended for electronic, computer, or other technologic aids in connection with the play of Class II games. This reduces the risk of misinterpretation whether intentional or unintentional. **Exposure of Non-Compliant System:** Non-compliant gaming systems have no basic requirements to ensure the integrity and security of Class II games and gaming revenue.
- 2. Control 547.2: What are the definitions for this part?** **Risks Mitigated by Control:** By defining the technical terms used in a standard, all stakeholders including manufacturers, testing laboratories, tribal governments, tribal gaming regulatory authorities, and operations all have a common understanding of the terms. Without definitions, the regulatory controls may be misinterpreted and incorrectly implemented exposing the gaming system to integrity and security risks. **Exposure of Non-Compliant System:** Non-Compliant systems have no reference of standardized terms. A component in one manufactures system may have different functionality from a component in another manufacturer's system with the name. This can also lead to confusion in operations and expose systems to additional risks.

Confidential 9 11/12/17

3. Control 547.3: Who is responsible for implementing these standards?

(a) Minimum standards. These are minimum standards and a TGRA may establish and implement additional technical standards that do not conflict with the standards set out in this part.

Risk Mitigated by Control:

Control 547.3 provides further definition and and clarity to the standard. While these are the minimum (baseline) controls, additional controls may be implemented provided that do not conflict or negate the minimum control.

Exposure of Non-Compliant System:

Non-compliant systems that have employed additional controls but do not meet the baseline or minimum requirements are likely to expose the system to catastrophic security and/or integrity risks. As an analogy, automobiles have a minimum requirement to have airbags. If an automobile was non-compliant but decided to employ additional controls such as forward collision warning, the results would be catastrophic. The automobile would warn of a collision but fail to protect the occupants because the minimum standard was not met.

(b) No limitation of technology. This part should not be interpreted to limit the use of technology or to preclude the use of technology not specifically referenced.

Risk Mitigated by Control:

Additional guidance is provided by defining that there are no limitations of technology.

Exposure of Non-Compliant System:

Without the minimum controls, the greater use of technology will expose the system to more vulnerabilities and risk of attack. The minimum technical standards are designed to provide the basic protection mechanisms to protect the system and thereby does not limit the use of technology.

(c) Only applicable standards apply. Gaming equipment and software must meet all applicable requirements of this part. For example, if a Class II gaming system lacks the ability to print or accept vouchers, then any standards that govern vouchers do not apply. These standards do not apply to associated equipment such as voucher and kiosk systems.

Confidential 10 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

Part C provides additional clarification and ensures that standards that are not applicable are introduced into the system. If a function does not exist, there is no need to employ a control that is not needed. **Exposure of Non-Compliant System:** Non-compliant systems adhere to no standard. As a result, all functions of the system are vulnerable to the threats the minimum standards mitigate.

(d) State jurisdiction. Nothing in this part should be construed to grant to a state jurisdiction over Class II gaming or to extend a state's jurisdiction over Class III gaming.

Risks Mitigated by Control:

No control required by the minimum technical standards would grant or extend state jurisdiction over the gaming system. This reduces the risk of conflicting regulatory requirements that could reduce the effectiveness and minimum controls.

Exposure of Non-Compliant System:

Non-compliant systems comply with no jurisdiction's regulations. As a result, these systems could violate law that may grant jurisdiction by state governments.

4. Control 547.4: What are the rules of general application for this part?

(a) Fairness. No Class II gaming system may cheat or mislead users. All prizes advertised must be available to win during the game. A test laboratory must calculate and/or verify the mathematical expectations of game play, where applicable, in accordance with the manufacturer stated submission. The results must be included in the test laboratory's report to the TGRA. At the request of the TGRA, the manufacturer must also submit the mathematical expectations of the game play to the TGRA.

Risk Mitigated by Control:

This control ensures the game is fair and not misleading or tricking game players. This control mitigates liability

Exposure of Non-Compliant System:

Non-compliant systems have no third party validation and maybe violating the expectations of the game. As a result, non-compliant systems increases the liability of the operator.

(b) Approved gaming equipment and software only. All gaming equipment and software used with Class II gaming systems must be identical in all respects to a prototype reviewed and tested by a testing laboratory and approved for use by the TGRA pursuant to § 547.5(a) through (c).

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

This control prevents the possibility of a system being deployed either knowingly or unintentional that has been altered from the configuration that was tested and certified.

Exposure of Non-Compliant System:

Non-compliant systems have no controls to ensure that configurations are not altered from the prototype tested. This increases the risk of systems violating the expectations and fairness of the game.

(c) Proper functioning. All gaming equipment and software used with Class II gaming systems must perform according to the manufacturer's design and operating specifications.

Risks Mitigated by Control:

This control ensures the system's design and operating specifications are accurate and represent the actual system.

Exposure of Non-Compliant System:

Non-compliant systems may operate and function differently than their design and operating specifications. These systems are more vulnerable to security and integrity risks as the system may intentionally or unintentionally be violating the operating behavior intended by the manufacturer.

5. Control 547.5: How does a tribal government, TGRA, or tribal gaming operation comply with this part? (a) Grandfathered gaming systems: Any Class II gaming system manufactured before November 10, 2008, that is not already certified pursuant to this sub-section or compliant with paragraph (c) of this section may be made available for use at any tribal gaming operation if:

(1) The TGRA submits the Class II gaming system software that affects the play of the Class II game, together with the signature verification required by § 547.8(f) to a testing laboratory recognized pursuant to paragraph (f) of this section within 120 days after October 22, 2012;

(2) The testing laboratory tests the submission to the standards established by § 547.8(b), § 547.8(f), § 547.14, and any additional technical standards adopted by the TGRA;

Confidential 12 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

- (3) The testing laboratory provides the TGRA with a formal written report setting forth and certifying to the findings and conclusions of the test;
- (4) The TGRA makes a finding, in the form of a certificate provided to the supplier or manufacturer of the Class II gaming system, that the Class II gaming system qualifies for grandfather status under the provisions of this section. A TGRA may make such a finding only upon receipt of a testing laboratory's report that the Class II gaming system is compliant with § 547.8(b), § 547.8(f), § 547.14, and any other technical standards adopted by the TGRA. If the TGRA does not issue the certificate, or if the testing laboratory finds that the Class II gaming system is not compliant with § 547.8(b), § 547.8(f), § 547.14, or any other technical standards adopted by the TGRA, then the gaming system must immediately be removed from play and not be utilized.
- (5) The TGRA retains a copy of any testing laboratory's report so long as the Class II gaming system that is the subject of the report remains available to the public for play; and
- (6) The TGRA retains a copy of any certificate of grandfather status so long as the Class II gaming system that is the subject of the certificate remains available to the public for play.
- (b) Grandfather provisions. All Class II gaming systems manufactured on or before November 10, 2008, that have been certified pursuant to paragraph (a) of this section, are grandfathered Class II gaming systems for which the following provisions apply:
- (1) Grandfathered Class II gaming systems may continue in operation for a period of ten years from November 10, 2008.
- (2) Grandfathered Class II gaming systems may only be used as approved by the TGRA. The TGRA must transmit its notice of that approval, identifying the grandfathered Class II gaming system and its components, to the Commission.
- (3) Remote communications may only be allowed if authorized by the TGRA.
- (4) As permitted by the TGRA, individual hardware or software components of a grandfathered Class II gaming system may be repaired or replaced to ensure proper functioning, security, or integrity of the grandfathered Class II gaming system.
- (5) All modifications that affect the play of a grandfathered Class II gaming system must be approved pursuant to paragraph (c) of this section, except for the following:

Confidential 13 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

- (i) Any software modifications that the TGRA finds will maintain or advance the Class II gaming system's overall compliance with this part or any applicable provisions of part 543 of this chapter, after receiving a new testing laboratory report that the modifications are compliant with the standards established by § 547.4(a), § 547.8(b), § 547.14, and any other standards adopted by the TGRA;
- (ii) Any hardware modifications that the TGRA finds will maintain or advance the Class II gaming system's overall compliance with this part or any applicable provisions of part 543 of this chapter; and
- (iii) Any other modification to the software of a grandfathered Class II gaming system that the TGRA finds will not detract from, compromise or prejudice:
 - (A) The proper functioning, security, or integrity of the Class II gaming system, and
 - (B) The gaming system's overall compliance with the requirements of this part or any applicable provisions of part 543 of this chapter.
- (iv) No such modification may be implemented without the approval of the TGRA. The TGRA must maintain a record of the modification so long as the Class II gaming system that is the subject of the modification remains available to the public for play and must make the record available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).
- (6) The player interface must exhibit information consistent with § 547.7(d) and any other information required by the TGRA.
- (7) If a grandfathered Class II gaming system is approved pursuant to paragraph (c) of this section, it ceases to be a grandfathered system and the restrictions of paragraph (a) and (b) of this section no longer apply.
- (c) Submission, testing, and approval—generally. Except as provided in paragraphs (b) and (d) of this section, a TGRA may not permit the use of any Class II gaming system, or any associated cashless system or voucher system or any modification thereto, in a tribal gaming operation unless:
 - (1) The Class II gaming system, cashless system, voucher system, or modification thereto has been submitted to a testing laboratory;

Confidential 14 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(2) The testing laboratory tests the submission to the standards established by: (i) This part;

(ii) Any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) The TGRA;

(3) The testing laboratory provides a formal written report to the party making the submission, setting forth and certifying its findings and conclusions, and noting compliance with any standard established by the TGRA pursuant to paragraph (c)(2)(iii) of this section;

(4) The testing laboratory's written report confirms that the operation of a player interface prototype has been certified that it will not be compromised or affected by electrostatic discharge, liquid spills, electromagnetic interference, radio frequency interference, or any other tests required by the TGRA;

(5) Following receipt of the testing laboratory's report, the TGRA makes a finding that the Class II gaming system, cashless system, or voucher system conforms to the standards established by:

(i) This part;

(ii) Any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) The TGRA.

(6) The TGRA retains a copy of the testing laboratory's report required by paragraph (c) of this section for as long as the Class II gaming system, cashless system, voucher system, or modification thereto that is the subject of the report remains available to the public for play in its tribal gaming operation.

(d) Emergency hardware and software modifications. (1) A TGRA, in its discretion, may permit the modification of previously approved hardware or software to be made available for play without prior laboratory testing or review if the modified hardware or software is:

(i) Necessary to correct a problem affecting the fairness, security, or integrity of a game

Confidential 15 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

or accounting system or any cashless system, or voucher system; or

(ii) Unrelated to game play, an accounting system, a cashless system, or a voucher system.

(2) If a TGRA authorizes modified software or hardware to be made available for play or use without prior testing laboratory review, the TGRA must thereafter require the hardware or software manufacturer to:

(i) Immediately advise other users of the same hardware or software of the importance and availability of the update;

(ii) Immediately submit the new or modified hardware or software to a testing laboratory for testing and verification of compliance with this part and any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) Immediately provide the TGRA with a software signature verification tool meeting the requirements of § 547.8(f) for any new or modified software.

(3) If a TGRA authorizes a software or hardware modification under this paragraph, it must maintain a record of the modification and a copy of the testing laboratory report so long as the Class II gaming system that is the subject of the modification remains available to the public for play and must make the record available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).

(e) Compliance by charitable gaming operations. This part does not apply to charitable gaming operations, provided that:

(1) The tribal government determines that the organization sponsoring the gaming operation is a charitable organization;

(2) All proceeds of the charitable gaming operation are for the benefit of the charitable organization;

(3) The TGRA permits the charitable organization to be exempt from this part;

(4) The charitable gaming operation is operated wholly by the charitable organization's employees or volunteers; and

Confidential 16 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(5) The annual gross gaming revenue of the charitable gaming operation does not exceed \$1,000,000.

(f) Testing laboratories. (1) A testing laboratory may provide the examination, testing, evaluating and reporting functions required by this section provided that:

(i) It demonstrates its integrity, independence and financial stability to the TGRA.

(ii) It demonstrates its technical skill and capability to the TGRA.

(iii) If the testing laboratory is owned or operated by, or affiliated with, a tribe, it must be independent from the manufacturer and gaming operator for whom it is providing the testing, evaluating, and reporting functions required by this section.

(iv) The TGRA:

(A) Makes a suitability determination of the testing laboratory based upon standards no less stringent than those set out in § 533.6(b)(1)(ii) through (v) of this chapter and based upon no less information than that required by § 537.1 of this chapter, or

(B) Accepts, in its discretion, a determination of suitability for the testing laboratory made by any other gaming regulatory authority in the United States.

(v) After reviewing the suitability determination and the information provided by the testing laboratory, the TGRA determines that the testing laboratory is qualified to test and evaluate Class II gaming systems.

(2) The TGRA must:

(i) Maintain a record of all determinations made pursuant to paragraphs (f)(1)(iii) and (f)(1)(iv) of this section for a minimum of three years and must make the records available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).

(ii) Place the testing laboratory under a continuing obligation to notify it of any adverse regulatory action in any jurisdiction where the testing laboratory conducts business.

(iii) Require the testing laboratory to provide notice of any material changes to the

Confidential 17 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

information provided to the TGRA.

Risk Mitigated by Control:

547.5 describes the conditions in which a grandfathered system may operate. This does not mitigate any risks and the ten year old grandfather rights exposes aging technology to greater risks without the protections of the minimum technical standards.

Exposure of Non-Compliant System:

Since grandfathered system do not employ the minimal technical standards, their exposure to security vulnerabilities and operational accuracy is compromised. The integrity of the hardware, software, operating parameters, and fairness of play is questionable due to the lack of baseline regulatory controls.

6. Control 547.6: What are the minimum technical standards for enrolling and enabling Class II gaming system components?

(a) General requirements. Class II gaming systems must provide a method to:

(1) Enroll and unenroll Class II gaming system components; (2) Enable and disable specific Class II gaming system components.

Risk Mitigated by Control:

This control ensures that there is a defined method by which a Class II gaming system identifies and establishes communications with an additional system component to allow for live gaming activity to take place on that component. This control reduces the risk of unauthorized communications between system components. This control ensures a proper process for disabling system components.

Exposure of Non-Compliant System:

Non-compliant systems may not have a defined method for identifying system components and establishing communications. Errors in identifying, establishing communications and disabling system components can expose the system to integrity and security risks.

(b) Specific requirements. Class II gaming systems must:

(1) Ensure that only enrolled and enabled Class II gaming system components participate in gaming; and

(2) Ensure that the default condition for components must be unenrolled and disabled.

Confidential 18 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risks Mitigated by Control:

The purpose of this control is to limit unauthorized requests to the server for any component that is not previously registered or enrolled. The control also requires a provision that requires the remote unenrollment or disabling of remote component. While we emphasize server, since it's the common type of attack, the control also applies to components within the game device itself.

Exposure of Non-Compliant System: A malicious intruder could connect a rogue device into the network or connect a form of hardware sniffer into the device to learn system behavior or tamper with it. Non-compliant systems are vulnerable to a variety of rogue and unauthorized component attacks.

7. Control 547.7: What are the minimum technical hardware standards applicable to Class II gaming systems?

(a) Printed circuit boards.

(1) Printed circuit boards that have the potential to affect the outcome or integrity of the game, and are specially manufactured or proprietary and not off-the-shelf, must display a unique identifier such as a part number and/or revision number, which must be updated to reflect new revisions or modifications of the board.

(2) Switches or jumpers on all circuit boards that have the potential to affect the outcome or integrity of any game, progressive award, financial instrument, cashless transaction, voucher transaction, or accounting records must be capable of being sealed.

Risk Mitigated by Control:

Off-the-shelf printed circuit boards may be vulnerable to common and well-known attack vectors. This control requires proprietary boards with unique identifiers. The risks of off-the-shelf attacks are reduced. The unique identifier indicates the proprietary manufacturer and version of the board. Security measure to prevent tampering with switches and jumpers are required.

Exposure of Non-Compliant System:

Non-compliant systems may deploy common off-the-shelf printed circuit boards that are vulnerable to well known attack vectors. The lack of unique identifiers on the board introduces accountability issues and reduces confidence in the system and the ability to identify the manufacturer and revision of the board. Furthermore, without compliance

Confidential 19 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

to the tamper-proof requirement, a threat actor with physical access to the system could compromise the integrity of the game by tampering with switches and jumpers.

(b) Electrostatic discharge. Class II gaming system components accessible to the public must be constructed so that they exhibit immunity to human body electrostatic discharges on areas exposed to contact. Static discharges of ± 15 kV for air discharges and ± 7.5 kV for contact discharges must not cause damage or inhibit operation or integrity of the Class II gaming system.

Risk Mitigated by Control:

This control ensures that systems components that are accessible to the public are immune immunity to human body electrostatic discharges. Electrostatic discharge can damage system components or affect the integrity of the game by introducing electronic error.

Exposure of Non-Compliant System:

Non-compliant system are vulnerable to damage, errors, and integrity threats due to electrostatic discharge.

(c) Physical enclosures. Physical enclosures must be of a robust construction designed to resist determined illegal entry. All protuberances and attachments such as buttons, identification plates, and labels must be sufficiently robust to avoid unauthorized removal.

Risk Mitigated by Control:

This control mitigates risks associated with physical intrusion to system components. Systems compliant with this minimum technical standard are tamper resistant.

Exposure of Non-Compliant System:

Non compliant systems could be tampered with physically through a breach of the enclosure or attachments and buttons. Without robust labeling, system identifications and other labeling could be altered.

(d) Player interface. The player interface must exhibit a serial number and date of manufacture and include a method or means to:

- (1) Display information to a player; and
- (2) Allow the player to interact with the Class II gaming system.

Risk Mitigated by Control:

Confidential 20 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

This control identifies the system to the player and improves the trustworthiness, accountability and fairness of play.

Exposure of Non-Compliant System:

Non-compliant systems can reduce player trust in the system due the lack of accountability information. Non-compliance with this control may prevent a player from interacting with the system.

(e) Account access components. A Class II gaming system component that reads account access media must be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components. In addition, the account access component:

- (1) Must be constructed so that physical tampering leaves evidence of such tampering; and
- (2) Must provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition.

Risk Mitigated by Control:

These controls prevent a system from being physically tampered with when account access media is used. Any attempt to tamper with the system is physically evident. These controls also ensure that the input from account access media are valid without error.

Exposure of Non-Compliant System:

Non-Compliant systems can be tampered with physically and there will be no physical evidence of tampering. Inputs can also be invalid without controls to ensure the validity and that the input is error-free.

(f) Financial instrument storage components. Any financial instrument storage components managed by Class II gaming system software must be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components.

Risk Mitigated by Control:

This controls ensures that system components that store tangible item of value (bills, coins, vouchers and coupons) are tamper resistant. Both the content and components of the storage component are physically protected by this control.

Exposure of Non-Compliant System:

Confidential 21 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Tangible items of value can be stolen from non-compliant systems. Additionally, storage system component can be physically damaged.

(g) Financial instrument acceptors. (1) Any Class II gaming system components that handle financial instruments and that are not operated under the direct control of an agent must:

(i) Be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components;

(ii) Be able to detect the entry of valid or invalid financial instruments and to provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition; and

(iii) Be constructed to permit communication with the Class II gaming system of the accounting information required by § 547.9(a) and by applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

(2) Prior to completion of a valid financial instrument transaction by the Class II gaming system, no monetary amount related to that instrument may be available for play. For example, credits may not be available for play until a financial instrument inserted into an acceptor is secured in the storage component.

(3) The monetary amount related to all valid financial instrument transactions by the Class II gaming system must be recorded as required by § 547.9(a) and the applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

Risk Mitigated by Control:

This control ensures that the system is protected from physical tampering of the Financial instrument acceptors and that the financial instrument is valid. The control also protects the system from timing attacks because no credit for play are provided until the financial instrument is validated and secured in the system storage compartment.

Exposure of Non-Compliant System:

Non compliant systems are vulnerable to physical tampering, invalid acceptance of fraudulent financial instruments, and timing attacks. A timing attack would cause the system to provide a game play before the financial instrument is validated and securely stored.

Confidential 22 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(h) Financial instrument dispensers. (1) Any Class II gaming system components that dispense financial instruments and that are not operated under the direct control of a tribal gaming operation agent must:

(i) Be located within a secure, locked and tamper-evident area or in a locked cabinet or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components;

(ii) Provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition; and

(iii) Be constructed to permit communication with the Class II gaming system of the accounting information required by § 547.9(a) and by applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

(2) The monetary amount related to all valid financial instrument transactions by the Class II gaming system must be recorded as required by § 547.9(a), the applicable provisions of part 543 of this chapter, and any TGRA regulations governing minimum internal control standards.

(i) Game Outcome Determination Components. Any Class II gaming system logic components that affect the game outcome and that are not operated under the direct control of a tribal gaming operation agent must be located within a secure, locked and tamper-evident area or in a locked cabinet or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components. DIP switches or jumpers that can affect the integrity of the Class II gaming system must be capable of being sealed by the TGRA.

Risk Mitigated by Control:

This control ensures that financial instrument dispensers are both tamper resistant and tamper evident. The system must have controls to detect valid, invalid, and error conditions and communicate with financial components. These controls protect the dispenser and the logic components

Exposure of Non-Compliant System:

A non-complaint system is vulnerable to physical tampering of the financial instrument dispenser. Without this control, the system may dispense financial instruments without the ability to detect invalid transactions and errors. The lack of this control can lead to financial losses.

Confidential 23 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(j) Door access detection. All components of the Class II gaming system that are locked in order to meet the requirements of this part must include a sensor or other methods to monitor an open door. A door open sensor, and its components or cables, must be secure against attempts to disable them or interfere with their normal mode of operation.

Risk Mitigated by Control:

This control protects the system from physical access and tampering through door access.

Exposure of Non-Compliant System:

Non-compliant system are vulnerable to physical tampering and sabotage due to the lack of sensors on door access and potentially vulnerable components and cables.

(k) Separation of functions/no limitations on technology. Nothing herein prohibits the account access component, financial instrument storage component, financial instrument acceptor, and financial instrument dispenser from being included within the same component or being separated into individual components.

Risk Mitigated by Control:

This standard allows system functions to be included into a single component or separated into individual components. No risks are mitigated by this requirement.

Exposure of Non-Compliant System:

This standard requirement does not introduce additional vulnerabilities to non-compliant as this standard allows functions to be integrated into a single component or distributed components.

8. Control 547.8: What are the minimum technical software standards applicable to Class II gaming systems?

(a) Player interface displays. (1) If not otherwise provided to the player, the player interface must display the following:

Confidential

(i) The purchase or wager amount; (ii) Game results; and (iii) Any player credit balance.

(2) Between plays of any game and until the start of the next play, or until the player selects a new game option such as purchase or wager amount or card

24 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

selection, whichever is earlier, if not otherwise provided to the player, the player interface must display:

- (i) The total purchase or wager amount and all prizes and total credits won for the last game played;
- (ii) The final results for the last game played; and (iii) Any default purchase or wager amount for the next play.

Risk Mitigated by Control:

This control mitigates the risk of incorrect information about the game and player status from being displayed on the player interface. This could be due to faulty or tampered software or hardware malfunction.

Exposure of Non-Compliant System:

Non-compliant systems are to faulty software, tampering, and hardware malfunctions. Without this control, the player interface can fail to display the required information.

(b) Game initiation and play. (1) Each game played on the Class II gaming system must follow and not deviate from a constant set of rules for each game provided to players pursuant to § 547.16. There must be no undisclosed changes of rules.

(2) The Class II gaming system may not alter or allow to be altered the card permutations used for play of a Class II game unless specifically chosen by the player prior to commitment to participate in the game. No duplicate cards may be sold for any common draw.

(3) No game play may commence, and no financial instrument or credit may be accepted on the affected player interface, in the presence of any fault condition that affects the outcome of the game, or while in test, audit, or lock-up mode.

(4) Each player must initiate his or her participation in the play of a game.

Risk Mitigated by Control:

The risk of Game initiation and play is a control to provide protection to the player under fair use. If a malfunction is detected, the game will not proceed.

Exposure of Non-Compliant System:

Non-compliant systems have no controls of Game initiation and play. Systems may malfunction and violate fairness of play regulations.

Confidential 25 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(c) Audit mode. (1) If an audit mode is provided, the Class II gaming system must, for those components actively involved in the audit:

(i) Provide all accounting functions required by § 547.9, by applicable provisions of any Commission regulations governing minimum internal control standards, and by any internal controls adopted by the tribe or TGRA;

(ii) Display player interface identification; and (iii) Display software version or game identification.

(2) Audit mode must be accessible by a secure method such as an agent PIN, key, or other auditable access control.

(3) Accounting function data must be accessible by an agent at any time, except during a payout, during a handpay, or during play.

(4) The Class II gaming system must disable financial instrument acceptance on the affected player interface while in audit mode, except during financial instrument acceptance testing.

Risk Mitigated by Control:

This control assures that systems accounting functions can be audited and that the proper identification information is displayed on the player interface.

Exposure of Non-Compliant System:

Non-compliant systems may not provide the ability to be audited and may not display the appropriate identification information. The lack of this control reduces confidence in the system and its accountability.

(d) Last game recall. The last game recall function must:

(1) Be retrievable at all times, other than when the recall component is involved in the play of a game, upon the operation of an external key-switch, entry of an audit card, or a similar method;

(2) Display the results of recalled games as originally displayed or in text representation so as to enable the TGRA or operator to clearly identify the sequences and results that occurred;

Confidential 26 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(3) Allow the Class II gaming system component providing game recall, upon return to normal game play mode, to restore any affected display to the positions, forms and values displayed before access to the game recall information; and

(4) Provide the following information for the current and previous four games played and must display:

(i) Play start time, end time, and date; (ii) The total number of credits at the start of play; (iii) The purchase or wager amount; (iv) The total number of credits at the end of play; (v) The total number of credits won as a result of the game recalled, and the value in dollars and cents for progressive prizes, if different; (vi) For bingo games and games similar to bingo, also display:

(A) The card(s) used by the player; (B) The identifier of the bingo game played; (C) The numbers or other designations drawn, in the order that they were drawn; (D) The numbers or other designations and prize patterns covered on each card; (E) All prizes won by the player, including winning patterns, if any; and (F) The unique identifier of the card on which prizes were won;

(vii) For pull-tab games only, also display:

(A) The result(s) of each pull-tab, displayed in the same pattern as on the tangible pull-tab; (B) All prizes won by the player; (C) The unique identifier of each pull tab; and

(D) Any other information necessary to fully reconstruct the current and four previous plays.

Risk Mitigated by Control:

This control ensures that an investigation can be conducted using the last game recall function.

Confidential 27 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Confidential

- (1) Display the information specified in § 547.11(b)(5)(ii) through (vi) for the last five vouchers or coupons printed and the last five vouchers or coupons accepted; and
- (2) Display a complete transaction history for the last five cashless transactions made and the last five cashless transactions accepted.

Risk Mitigated by Control:

This control ensures that an investigation can be conducted using the “Voucher and credit transfer recall” function.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of not being able to recall the “Voucher and credit transfer recall” function at any given time is that the system has being tampered with to hide voucher and credit results that could be obvious to an investigation.

(f) Software signature verification. The manufacturer or developer of the Class II gaming system must provide to the testing laboratory and to the TGRA an industry-standard methodology, acceptable to the TGRA, for verifying the Class II gaming system game software. For example, for game software stored on rewritable media, such methodologies include signature algorithms and hashing formulas such as SHA-1.

Risk Mitigated by Control:

This control ensures through digital signatures (Authenticity and Integrity) or hashing algorithms (Integrity) that the manufacturers software truly originated from the developer and that is has not been modified intentionally or unintentionally.

Exposure of Non-Compliant System:

28 11/12/17

Exposure of Non-Compliant System:

Non-compliant systems are at risk of not being able to recall the “Last game recall” function at any given time is that the system has being tampered with to hide payouts or odd results that could be obvious to an investigation. The lack of “Last game recall” controls may lead to financial losses.

(e) Voucher and credit transfer recall. Notwithstanding the requirements of any other section in this part, a Class II gaming system must have the capacity to:

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Non-compliant systems are vulnerable to fraudulent or imposter software submissions and software that may have been modified intentionally or by error.

(g) Test, diagnostic, and demonstration modes. If test, diagnostic, and/or demonstration modes are provided, the Class II gaming system must, for those components actively involved in the test, diagnostic, or demonstration mode:

- (1) Clearly indicate when that component is in the test, diagnostic, or demonstration mode;
- (2) Not alter financial data on that component other than temporary data; (3) Only be available after entering a specific mode;
- (4) Disable credit acceptance and payment unless credit acceptance or payment is being tested; and
- (5) Terminate all mode-specific functions upon exiting a mode.

Risk Mitigated by Control:

The control for the Test, diagnostic, and demonstration modes (if provided) specifies that no payment can be accepted and the display should indicate the mode. This control prevents the alternation of financial data while in test, diagnostic, and demonstration modes.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to financial fraud as they do not have controls to prevent manipulation of financial data while in test, diagnostic, and demonstration modes.

(h) Multigame. If multiple games are offered for player selection at the player interface, the player interface must:

- (1) Provide a display of available games; (2) Provide the means of selecting among them; (3) Display the full amount of the player's credit balance; (4) Identify the game selected or being played; and (5) Not force the play of a game after its selection.

Confidential 29

11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

The Multigame control relates to player protection, to make sure that their balance is carried over from game to game.

Exposure of Non-Compliant System:

Non-compliant systems may violate player protection rules losing player information and balance information in multi game mode.

(i) Program interruption and resumption. The Class II gaming system software must be designed so that upon resumption following any interruption, the system:

(1) Is able to return to a known state; (2) Must check for any fault condition; (3) Must verify the integrity of data stored in critical memory; (4) Must return the purchase or wager amount to the player in accordance with

the rules of the game; and (5) Must detect any change or corruption in the Class II gaming system software.

Risk Mitigated by Control:

This control ensures that the system fails and recovers in a safe and predictable manner.

Exposure of Non-Compliant System:

Non-compliant systems may fail to an unknown state, fail to detect failure conditions and produce financial accounting errors.

(j) Class II gaming system components acting as progressive controllers. This paragraph applies to progressive controllers and components acting as progressive controllers in Class II gaming systems.

(1) Modification of progressive parameters must be conducted in a secure manner approved by the TGRA. Such parameters may include: (i) Increment value; (ii) Secondary pool increment(s);

(iii) Reset amount(s); (iv) Maximum value(s); and (v) Identity of participating player interfaces.

(2) The Class II gaming system component or other progressive controller must provide a means of creating a progressive balancing report for each progressive link it controls. At a minimum, that report must provide balancing of the changes of the progressive amount, including progressive prizes won, for all participating player interfaces versus

Confidential 30 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

current progressive amount(s), plus progressive prizes. In addition, the report must account for, and not be made inaccurate by, unusual events such as:

(i) Class II gaming system critical memory clears; (ii) Modification, alteration, or deletion of progressive prizes; (iii) Offline equipment; or (iv) Multiple site progressive prizes.

Risk Mitigated by Control:

This control related Class II gaming system components acting as progressive controllers indicates that the rules for these complex games are very strict and the reporting module must account for this complex progressive mode to avoid missing any tampering or software defect.

Exposure of Non-Compliant System:

Non-compliant systems may prevent the auditing of progressive transactions. These systems are at risk of tampering and violating fairness of play.

(k) Critical memory. (1) Critical memory may be located anywhere within the Class II gaming system. Critical memory is any memory that maintains any of the following data:

(i) Accounting data; (ii) Current credits; (iii) Configuration data; (iv) Last game play recall information required by paragraph (d) of this section; (v) Game play recall information for the current game play, if incomplete;

(vi) Software state (the last normal state software was in before interruption); (vii) RNG seed(s), if necessary for maintaining integrity; (viii) Encryption keys, if necessary for maintaining integrity; (ix) Progressive prize parameters and current values;

(x) The five most recent financial instruments accepted by type, excluding coins and tokens; (xi) The five most recent financial instruments dispensed by type, excluding coins and tokens; and

(xii) The five most recent cashless transactions paid and the five most recent cashless transactions accepted.

(2) Critical memory must be maintained using a methodology that enables errors to be identified and acted upon. All accounting and recall functions must be verified as necessary to ensure their ongoing integrity.

Confidential 31 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(3) The validity of affected data stored in critical memory must be checked after each of the following events:

(i) Every restart; (ii) Each attendant paid win; (iii) Each attendant paid progressive win; (iv) Each sensed door closure; and (v) Every reconfiguration, download, or change of prize schedule or denomination requiring operator intervention or action.

Risk Mitigated by Control:

This control ensures the validity and integrity of system transactions and data in critical memory.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to critical memory errors: storing faulty data, losing stored data or corrupted memory system, or retrieving incorrect data. All these could occur due to hardware or software malfunction, or due to malicious software tampering.

(l) Secured access. Class II gaming systems that use a logon or other means of secured access must include a user account lockout after a predetermined number of consecutive failed attempts to access the Class II gaming system.

Risk Mitigated by Control:

This access control is to minimize the risk of potential intruders trying to brute force the logon account by trying many combinations to guess the password. This control sets a clipping level that after a number of invalid tries, will lockout the account.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to brute force login attacks.

9. Control 547.9: What are the minimum technical standards for Class II gaming system accounting functions?

(a) Required accounting data. The following minimum accounting data, however named, must be maintained by the Class II gaming system:

(1) Amount In: The total value of all financial instruments and cashless transactions accepted by the Class II gaming system. Each type of financial instrument accepted by the Class II gaming system must be tracked independently per financial instrument

Confidential 32 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

acceptor, and as required by applicable requirements of TGRA regulations that meet or exceed the minimum internal control standards at 25 CFR part 543.

(2) Amount Out: The total value of all financial instruments and cashless transactions paid by the Class II gaming system, plus the total value of attendant pay. Each type of financial instrument paid by the Class II Gaming System must be tracked independently per financial instrument dispenser, and as required by applicable requirements of TGRA regulations that meet or exceed the minimum internal control standards at 25 CFR part 543.

Risk Mitigated by Control:

This control is both an accounting and audit control to monitor system financial transactions.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to financial fraud due to the lack of accounting audit capabilities.

(b) Accounting data storage. If the Class II gaming system electronically maintains accounting data:

(1) Accounting data must be stored with at least eight decimal digits.

(2) Credit balances must have sufficient digits to accommodate the design of the game.

(3) Accounting data displayed to the player may be incremented or decremented using visual effects, but the internal storage of this data must be immediately updated in full.

(4) Accounting data must be updated upon the occurrence of the relevant accounting event.

(5) Modifications to accounting data must be recorded, including the identity of the person(s) making the modifications, and be reportable by the Class II gaming system.

Risk Mitigated by Control:

This control ensures proper accounting transaction, precision of the data and accounting systems.

Exposure of Non-Compliant System:

Non-compliant systems cannot ensure that accounting data is properly stored, the precision of the data, the logging of persons modifying accounting data, and ensuring

Confidential 33 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

the transactions are recorded upon a relevant event.

(c) Rollover. Accounting data that rolls over to zero must not corrupt data.

Risk Mitigated by Control:

This control ensures when data rolls over to zero no data corruption occurs.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of corrupting data.

(d) Credit balance display and function. (1) Any credit balance maintained at the player interface must be prominently displayed at all times except:

(i) In audit, configuration, recall and test modes; or (ii) Temporarily, during entertaining displays of game results.

(2) Progressive prizes may be added to the player's credit balance provided that: (i) The player credit balance is maintained in dollars and cents; (ii) The progressive accounting data is incremented in number of credits; or (iii) The prize in dollars and cents is converted to player credits or transferred to

the player's credit balance in a manner that does not mislead the player or cause accounting imbalances.

(3) If the player credit balance displays in credits, but the actual balance includes fractional credits, the Class II gaming system must display the fractional credit when the player credit balance drops below one credit.

Risk Mitigated by Control:

This control ensures that any credit balance maintained at the player interface must be prominently displayed.

Exposure of Non-Compliant System:

Non-compliant systems may violate fairness of play by not properly displaying credit balance at the required precision.

10. Control 547.10: What are the minimum standards for Class II gaming system critical events?

(a) Fault events. (1) The following are fault events that must be capable of being recorded by the Class II gaming system:

(i) Component fault

Confidential 34 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Reported when a fault on a component is detected. When possible, this event message should indicate what the nature of the fault is.

(ii) Financial storage component full Reported when a financial instrument acceptor or dispenser includes storage, and it becomes full. This event message must indicate what financial storage component is full. (iii) Financial output component empty Reported when a financial instrument dispenser is empty. The event message must indicate which financial output component is affected, and whether it is empty. (iv) Financial component fault Reported when an occurrence on a financial component results in a known fault state.

(v) Critical memory error Some critical memory error has occurred. When a non-correctable critical memory error has occurred, the data on the Class II gaming system component can no longer be considered reliable. Accordingly, any game play on the affected component must cease immediately, and an appropriate message must be displayed, if possible.

(vi) Progressive communication fault If applicable; when communications with a progressive controller component is in a known fault state.

(vii) Program storage medium fault The software has failed its own internal security check or the medium itself has some fault. Any game play on the affected component must cease immediately, and an appropriate message must be displayed, if possible.

(2) The occurrence of any event identified in paragraph (a)(1) of this section must be recorded.

(3) Upon clearing any event identified in paragraph (a)(1) of this section, the Class II gaming system must:

(i) Record that the fault condition has been cleared; (ii) Ensure the integrity of all related accounting data; and

(iii) In the case of a malfunction, return a player's purchase or wager according to the rules of the game.

Confidential 35 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

This control is critical to ensuring the integrity of the systems by detecting and logging fault events.

Exposure of Non-Compliant System:

Non-compliant systems may be unable to record fault events. This violates the security, integrity and accounting reliability of the system.

(b)Door open/close events.

(1) In addition to the requirements of paragraph (a)(1) of this section, the Class II gaming system must perform the following for any component affected by any sensed door open event: (i) Indicate that the state of a sensed door changes from closed to open or opened to closed;

(ii) Disable all financial instrument acceptance, unless a test mode is entered; (iii) Disable game play on the affected player interface; (iv) Disable player inputs on the affected player interface, unless test mode is entered; and (v) Disable all financial instrument disbursement, unless a test mode is entered. (2) The Class II gaming system may return the component to a ready to play state when all sensed doors are closed.

Risk Mitigated by Control:

This control ensures that the system will halt play and financial transactions when a door sensor is active.

Exposure of Non-Compliant System:

Non-compliant systems may not detect a door open sensor and allow play and financial transactions to continue. The lack of this control may allow fraudulent play and financial transactions while the system is in a physical insecure state.

(c) Non-fault events. The following non-fault events are to be acted upon as described below, if applicable:

Event Definition

(1) Player interface off during play Indicates power has been lost during game play. This condition must be reported by the affected component(s). (2) Player interface power on Indicates the player interface has been turned on. This condition must be reported by the affected component(s).

Confidential 36 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(3) Financial instrument storage component container/stacker removed Indicates that a financial instrument storage container has been removed. The event message must indicate which storage container was removed.

Risk Mitigated by Control:

This control ensures that non-fault events are properly reported and the components affected are indicated.

Exposure of Non-Compliant System:

Non-compliant systems may not report non-fault events. The lack of this control reduces the integrity of the system by not reporting non-fault events.

11. Control 547.11: What are the minimum technical standards for money and credit handling?

(a) Credit acceptance, generally. (1) Upon any credit acceptance, the Class II gaming system must register the correct number of credits on the player's credit balance. (2) The Class II gaming system must reject financial instruments deemed invalid.

Risk Mitigated by Control:

This control ensures the system correctly registers valid player credits and rejects financial instruments deemed invalid.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of accepting invalid financial instruments and not properly registering player credits.

(b) Credit redemption, generally. (1) For cashable credits on a player interface, players must be allowed to cash out and/or redeem those credits at the player interface except when that player interface is:

(i) Involved in the play of a game; (ii) In audit mode, recall mode or any test mode; (iii) Detecting any sensed door open condition; (iv) Updating the player credit balance or total win accounting data; or (v) Displaying a fault condition that would prevent cash-out or credit redemption. In this case a fault indication must be displayed.

(2) For cashable credits not on a player interface, the player must be allowed to cash out and/or redeem those credits at any time.

Confidential 37 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

- (3) A Class II gaming system must not automatically pay an award subject to mandatory tax reporting or withholding.
- (4) Credit redemption by voucher or coupon must conform to the following: (i) A Class II gaming system may redeem credits by issuing a voucher or coupon when it communicates with a voucher system that validates the voucher or coupon. (ii) A Class II gaming system that redeems credits by issuing vouchers and coupons must either:
- (A) Maintain an electronic record of all information required by paragraphs (b)(5)(ii) through (vi) of this section; or
- (B) Generate two identical copies of each voucher or coupon issued, one to be provided to the player and the other to be retained within the electronic player interface for audit purposes.
- (5) Valid vouchers and coupons from a voucher system must contain the following: (i) Tribal gaming operation name and location;
- (ii) The identification number of the Class II gaming system component or the player interface number, as applicable;
- (iii) Date and time of issuance;
- (iv) Alpha and numeric dollar amount;
- (v) A sequence number;
- (vi) A validation number that:
- (A) Is produced by a means specifically designed to prevent repetition of validation numbers; and
- (B) Has some form of checkcode or other form of information redundancy to prevent prediction of subsequent validation numbers without knowledge of the checkcode algorithm and parameters;
- (vii) For machine-readable vouchers and coupons, a bar code or other form of machine readable representation of the validation number, which must have enough redundancy

Confidential 38 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

and error checking to ensure that 99.9% of all misreads are flagged as errors; (viii) Transaction type or other method of differentiating voucher and coupon types; and (ix) Expiration period or date. (6) Transfers from an account may not exceed the balance of that account.

(7) For Class II gaming systems not using dollars and cents accounting and not having odd cents accounting, the Class II gaming system must reject any transfers from voucher systems or cashless systems that are not even multiples of the Class II gaming system denomination.

(8) Voucher systems must include the ability to report redemptions per redemption location or user.

Risk Mitigated by Control:

This control ensures rules and conditions are followed for cashable credit and vouchers.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to invalid cashable payments, fraudulent vouchers and accounting errors due to their lack of rules based controls.

12. Control 547.12: What are the minimum technical standards for downloading on a Class II gaming system?

(a) Downloads. (1) Downloads are an acceptable means of transporting approved content, including, but not limited to software, files, data, and prize schedules. (2) Downloads must use secure methodologies that will deliver the download data without alteration or modification, in accordance with § 547.15(a).

(3) Downloads conducted during operational periods must be performed in a manner that will not affect game play. (4) Downloads must not affect the integrity of accounting data. (5) The Class II gaming system must be capable of providing:

(i) The time and date of the initiation of the download; (ii) The time and date of the completion of the download; (iii) The Class II gaming system components to which software was downloaded; (iv) The version(s) of download package and any software downloaded. Logging

of the unique software signature will satisfy this requirement; (v) The outcome of any software verification following the download (success or

failure); and

Confidential 39 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(vi) The name and identification number, or other unique identifier, of any individual(s) conducting or scheduling a download.

(b) Verifying downloads. Downloaded software on a Class II gaming system must be capable of being verified by the Class II gaming system using a software signature verification method that meets the requirements of § 547.8(f).

Risk Mitigated by Control:

This control requires the secure transmission of software, including creating audit records and verification to ensure no tampering occurred. An audit trail is created tracking the downloads integrity, source, destination, timestamps, and other identifiers.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to downloads that may have been altered, modified, or from unreliable sources. The lack of audit tracking could lead to undesirable behavior from malicious downloads in the non-compliant system.

13. Control 547.13: What are the minimum technical standards for program storage media?

(a) Removable program storage media. All removable program storage media must maintain an internal checksum or signature of its contents. Verification of this checksum or signature is to be performed after every restart. If the verification fails, the affected Class II gaming system component(s) must lock up and enter a fault state.

Risk Mitigated by Control:

This control prevents removable program storage from invalid sources and from the data being intentionally or unintentionally modified or altered. Signature or checksum failures results in a fault state to protect the system from damage.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of being infected by malicious content on removable program storage. This is a critical control to prevent system damage.

(b) Non-rewritable program storage media. (1) All EPROMs and Programmable Logic Devices that have erasure windows must be fitted with covers over their erasure windows.

(2) All unused areas of EPROMs must be written with the inverse of the erased state (zero bits (00 hex) for most EPROMs), random data, or repeats of the program data.

Confidential 40 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

- (3) Flash memory storage components intended to have the same logical function as ROM, must be write-protected or otherwise protected from unauthorized modification.
- (4) The write cycle must be closed or finished for all CD-ROMs such that it is not possible to write any further data to the CD.
- (5) Write protected hard disks are permitted if the hardware means of enabling the write protect is easily viewable and can be sealed in place. Write protected hard disks are permitted using software write protection verifiable by a testing laboratory.

Risk Mitigated by Control:

This control protects non-rewritable program storage media from unauthorized modification or storage of malicious content.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to malicious software and/or unauthorized modification of data on non-rewritable program storage media.

(c) Writable and rewritable program storage media. (1) Writable and rewritable program storage, such as hard disk drives, Flash memory, writable CD-ROMs, and writable DVDs, may be used provided that the software stored thereon may be verified using the mechanism provided pursuant to § 547.8(f).

(2) Program storage must be structured so there is a verifiable separation of fixed data (such as program, fixed parameters, DLLs) and variable data.

Risk Mitigated by Control:

This control assures the integrity of writable and rewritable program storage media through the use of signatures and checksum to validate the source and to prevent modification or alteration.

Exposure of Non-Compliant System:

As with other forms of program storage media, non-compliant systems are vulnerable to malicious software and unauthorized modifications of data due to the lack of this control.

(d) Identification of program storage media. All program storage media that is not rewritable in circuit, (EPROM, CD-ROM) must be uniquely identified, displaying:

(1) Manufacturer; (2) Program identifier;

Confidential 41 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(3) Program version number(s); and (4) Location information, if critical (socket position 3 on the printed circuit board).

Risk Mitigated by Control:

This control is used to track and clearly identify the source and content of program storage media.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of using invalid program storage media due to the lack of labeling controls.

14. Control 547.14; What are the minimum technical standards for electronic random number generation?

(a) Properties. All RNGs must produce output having the following properties: (1) Statistical randomness;

(2) Unpredictability; and (3) Non-repeatability.

Risk Mitigated by Control:

This control reduces the risks associated with prediction attacks by ensuring sufficiently random numbers are used by the gaming system.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of not producing sufficiently random numbers. An attacker could calculate and predict the next move or play sequence in the game.

(b) Statistical randomness. (1) Numbers or other designations produced by an RNG must be statistically random individually and in the permutations and combinations used in the application under the rules of the game. For example, if a bingo game with 75 objects with numbers or other designations has a progressive winning pattern of the five numbers or other designations on the bottom of the card, and the winning of this prize is defined to be the five numbers or other designations that are matched in the first five objects drawn, the likelihood of each of the 75C5 combinations are to be verified to be statistically equal.

(2) Numbers or other designations produced by an RNG must pass the statistical tests for randomness to a 99% confidence level, which may include: (i) Chi-square test; (ii) Runs test (patterns of occurrences must not be recurrent); and

(iii) Serial correlation test potency and degree of serial correlation (outcomes must be

Confidential 42 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

independent from the previous game). (iv) Equi-distribution (frequency) test; (v) Gap test; (vi) Poker test;

(vii) Coupon collector's test; (viii) Permutation test; (ix) Spectral test; or (x) Test on subsequences.

Risk Mitigated by Control:

This control reduces the risk of a weak RNG producing predictable values.

Exposure of Non-Compliant System:

Non-compliant systems may produce predictable RNG values. A threat actor may discover repeatable pattern in a game to exploit it during game play.

(c) Unpredictability. (1) It must not be feasible to predict future outputs of an RNG, even if the algorithm and the past sequence of outputs are known.

(2) Unpredictability must be ensured by reseeding or by continuously cycling the RNG, and by providing a sufficient number of RNG states for the applications supported.

(3) Re-seeding may be used where the re-seeding input is at least as statistically random as, and independent of, the output of the RNG being re-seeded.

Risk Mitigated by Control:

This control reduces the risks associated with future outputs of a RNG.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of predictability in the RNG.

(d) Non-repeatability. The RNG may not be initialized to reproduce the same output stream that it has produced before, nor may any two instances of an RNG produce the same stream as each other. This property must be ensured by initial seeding that comes from:

(1) A source of “true” randomness, such as a hardware random noise generator; or

(2) A combination of timestamps, parameters unique to a Class II gaming system, previous RNG outputs, or other, similar method.

Confidential 43 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

This controls reduces the probability the RNG will produce a repeatable output. Seeding from a reliable source of randomness is required.

Exposure of Non-Compliant System:

Non-compliant systems are likely to product repeatability in the RNG is these seeding requirements are not met.

(e) General requirements. (1) Software that calls an RNG to derive game outcome events must immediately use the output returned in accordance with the game rules.

(2) The use of multiple RNGs is permitted as long as they operate in accordance with this section.

(3) RNG outputs must not be arbitrarily discarded or selected.

(4) Where a sequence of outputs is required, the whole of the sequence in the order generated must be used in accordance with the game rules.

(5) The Class II gaming system must neither adjust the RNG process or game outcomes based on the history of prizes obtained in previous games nor use any reflexive software or secondary decision that affects the results shown to the player or game outcome.

Risk Mitigated by Control:

This control mandates the usage of RNG outputs to reduce reduce observation attacks based on analysis of historic RNG outputs.

Exposure of Non-Compliant System:

Systems that are not compliant with the RNG general requirements are at risk of an attacker potentially install monitoring software to analyze historical or unused values in order to predict future results.

(f) Scaling algorithms and scaled numbers. An RNG that provides output scaled to given ranges must:

(1) Be independent and uniform over the range;

(2) Provide numbers scaled to the ranges required by game rules, and notwithstanding the requirements of paragraph (e)(3) of this section, may discard numbers that do not map uniformly onto the required range but must use the first number in sequence that

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

does map correctly to the range; (3) Be capable of producing every possible outcome of a game according to its rules; and

(4) Use an unbiased algorithm. A scaling algorithm is considered to be unbiased if the measured bias is no greater than 1 in 50 million.

Risk Mitigated by Control:

This control ensures that scaling algorithms and scaled numbers do not produce predictable patterns.

Exposure of Non-Compliant System:

The risk of non-compliant systems is predictability in the RNG that an attacker could use to calculate and predict the next move or play sequence in the game.

15. Control 547.15: What are the minimum technical standards for electronic data communications between system components?

(a) Sensitive data. Communication of sensitive data must be secure from eavesdropping, access, tampering, intrusion or alteration unauthorized by the TGRA. Sensitive data includes, but is not limited to:

(1) RNG seeds and outcomes; (2) Encryption keys, where the implementation chosen requires transmission of keys; (3) PINs; (4) Passwords; (5) Financial instrument transactions; (6) Transfers of funds; (7) Player tracking information; (8) Download Packages; and (9) Any information that affects game outcome.

Risk Mitigated by Control:

This control ensures the protection of sensitive data in communication channels. Protection of the confidentiality and integrity of the data in transit.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of exposing critical data in transit. The confidentiality and integrity of the data is compromised with these controls.

Confidential 45 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(b) Wireless communications. (1) Wireless access points must not be accessible to the general public.

(2) Open or unsecured wireless communications are prohibited.

(3) Wireless communications must be secured using a methodology that makes eavesdropping, access, tampering, intrusion or alteration impractical. By way of illustration, such methodologies include encryption, frequency hopping, and code division multiplex access (as in cell phone technology).

Risk Mitigated by Control:

This control ensures the secure transmission of data over and monitoring of wireless communications.

Exposure of Non-Compliant System:

Non-compliant systems expose wireless communication to easily perpetrated and well known attacks that compromise the confidentiality and integrity data.

(c) Methodologies must be used that will ensure the reliable transfer of data and provide a reasonable ability to detect and act upon any corruption of the data.

Risk Mitigated by Control:

This control requires ensures the reliable transmission of data with the ability to detect and recover from data transmission corruption whether intentional or unintentional.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of receiving and transmitting data that has been modified by system errors or malicious actors.

(d) Class II gaming systems must record detectable, unauthorized access or intrusion attempts.

Risk Mitigated by Control:

This detective control ensures intrusions will be detected and logged.

Exposure of Non-Compliant System:

Non-compliant systems would allow intrusions to go undetected leading to additional system and data breaches.

(e) Remote communications may only be allowed if authorized by the TGRA. Class II gaming systems must have the ability to enable or disable remote access, and the

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

default state must be set to disabled.

Risk Mitigated by Control:

This control reduces the risk associated with remote communication by providing mechanisms to disable or remove remote access to keep the system protected.

Exposure of Non-Compliant System:

Non-compliant systems are at risk on remote communication not being disabled. Open remote communication channels could be used by a threat actor to gain unauthorized access to gaming consoles or servers.

(f) Failure of data communications must not affect the integrity of critical memory.

Risk Mitigated by Control:

This control ensures that critical memory integrity will be maintained even if there is loss of communications.

Exposure of Non-Compliant System:

Non-compliant systems are at risk of corrupting the integrity of critical memory during a communications failure.

(g) The Class II gaming system must log the establishment, loss, and re-establishment of data communications between sensitive Class II gaming system components.

Risk Mitigated by Control:

This control ensures that all data communications between system components are logged.

Exposure of Non-Compliant System:

Non-compliant systems will not log the establishment, loss, and re-establishment of data communications between system components. This increases the risk of undetected intrusion and unauthorized access.

16. Control 547.16: What are the minimum standards for game artwork, glass, and rules?

(a) Rules, instructions, and prize schedules, generally. The following must at all times be displayed or made readily available to the player upon request: (1) Game name, rules, and options such as the purchase or wager amount stated clearly and unambiguously;

Confidential 47 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

(2) Denomination;

(3) Instructions for play on, and use of, the player interface, including the functions of all buttons; and

(4) A prize schedule or other explanation, sufficient to allow a player to determine the correctness of all prizes awarded, including:

(i) The range and values obtainable for any variable prize; (ii) Whether the value of a prize depends on the purchase or wager amount; and (iii) The means of division of any pari-mutuel prizes; but

(iv) For Class II Gaming Systems, the prize schedule or other explanation need not state that subsets of winning patterns are not awarded as additional prizes (for example, five in a row does not also pay three in a row or four in a row), unless there are exceptions, which must be clearly stated.

Risk Mitigated by Control:

This control ensures fair play and full disclosure to the player.

Exposure of Non-Compliant System:

Non-compliant systems may not disclose information to Players thereby reducing trust and acceptance of the system.

(b) Disclaimers. The Player Interface must continually display: (1) “Malfunctions void all prizes and plays” or equivalent; and (2) “Actual Prizes Determined by Bingo (or other applicable Class II game) Play. Other Displays for Entertainment Only” or equivalent.

Risk Mitigated by Control:

This control provides awareness to the player of all disclaimers in the interest of fair play.

Exposure of Non-Compliant System:

Non-compliant systems violates requirements to display disclaimers.

(c) Odds notification. If the odds of winning any advertised top prize exceeds 100 million to one, the Player Interface must display: “Odds of winning the advertised top prize exceeds 100 million to one” or equivalent.

Confidential 48 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

Risk Mitigated by Control:

The only risk is the player not knowing the odds of the game. More like a legal disclaimer to inform the consumer, not a security risk.

Exposure of Non-Compliant System:

The exposure of older systems not complying with this control is higher than in new systems that have this built in functionality installed. In any event, minimal exposure.

17. Control 547.17: How does a TGRA apply to implement an alternate minimum standard to those required by this part?

(a) TGRA approval. (1) A TGRA may approve an alternate standard from those required by this part if it has determined that the alternate standard will achieve a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace. A gaming operation may implement an alternate standard upon TGRA approval subject to the Chair's decision pursuant to paragraph (b) of this section.

(2) For each enumerated standard for which the TGRA approves an alternate standard, it must submit to the Chair within 30 days a detailed report, which must include the following:

(i) An explanation of how the alternate standard achieves a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace; and

(ii) The alternate standard as approved and the record on which the approval is based.

(3) In the event that the TGRA or the tribe's government chooses to submit an alternate standard request directly to the Chair for joint government to government review, the TGRA or tribal government may do so without the approval requirement set forth in paragraph (a)(1) of this section.

Risk Mitigated by Control:

TGRA may submit a new stronger standard than the minimal technical standards.

Exposure of Non-Compliant System:

Non-compliant systems manufactured before November 10, 2008 are at risk of not having the technology required to meet the requirements of alternate standards.

(b) Chair review. (1) The Chair may approve or object to an alternate standard approved by a TGRA.

Confidential 49 11/12/17

Coalition for Fair Gaming, LLC Class II Gaming Systems: Risk Analysis Report

- (2) If the Chair approves the alternate standard, the Tribe may continue to use it as authorized by the TGRA.
- (3) If the Chair objects to the alternate standard, the operation may no longer use the alternate standard and must follow the relevant technical standard set forth in this part.
- (4) Any objection by the Chair must be in written form with an explanation why the alternate standard as approved by the TGRA does not provide a level of security or integrity sufficient to accomplish the purpose of the standard it is to replace.
- (5) If the Chair fails to approve or object in writing within 60 days after the date of receipt of a complete submission, the alternate standard is considered approved by the Chair. The Chair may, upon notification to the TGRA, extend this deadline an additional 60 days.

Risk Mitigated by Control:

This requirement outlines chair approval of alternate standards.

Exposure of Non-Compliant System:

Non-compliant systems are not likely to meet alternate standards.

- (c) Appeal of Chair decision. A TGRA may appeal the Chair's decision pursuant to 25 CFR chapter III, subchapter H.

Risk Mitigated by Control:

This requirement addresses chair decision appeal

Exposure of Non-Compliant System:

Not relevant to non-compliant systems.

Confidential 50 11/12/17