# Vulnerability Management Continuous Monitoring

(Operating System Patch Management)
Audit Services

February 28, 2019

bclc

# Table of Contents

bclc

# Transmittal Letter

April 24, 2019

Don Lacey
Director Technology & Operations Service
74 West Seymour Street
Kamloops, BC V2C 1E2

Dear Mr. Lacey:

**Re:** **Vulnerability Management Continuous Monitoring (Part 1: Operating System Patch Management)**

Attached is the Audit Services' report on the above audit.

Our findings herein include four recommendations that address four moderate risk topics. Management has agreed with our recommendations and developed appropriate response plans to address each item identified.

We thank the management and staff of the Business Technology and Cybersecurity for their cooperation and assistance during this audit.

Sincerely,

s 22

Gurmit Aujla CPA, CA,\CIA, CRISC, CRMA
Director, Internal Audit

cc:     Pat Davis, Chief Information Officer
        Rob Kroeker, Chief Compliance Officer & VP Legal, Compliance, Security
        Kevin Sweeney, Director Security, Privacy and Compliance

# Introduction

Cybersecurity Risk is identified as one of the top 10 strategic risks within BCLC's Risk Universe. While the risk of breaches and attacks can materialize in a number of ways, one example is Equifax's high-profile breach[1] in 2017 that exposed personal information, seemingly as a result of the company's failure to implement the appropriate patch in a timely manner.

As such, the work by Business Technology (BT) and Legal, Compliance, Security divisions to build a comprehensive cybersecurity strategy is critical to the planned risk treatment. In particular, vulnerability management, and specifically patch management, a practice intended to proactively prevent potential exploitation of IT vulnerabilities, are key operational controls to help mitigate such risks. In April 2018, Audit Services conducted a follow-up from a prior 2016 engagement and reported on progress being made in the areas of:

- Vulnerability Management oversight;
- Anti-virus deployment; as well as,
- Improvements to operating systems patch deployment (now on a 30-day patch cycle) and patch management reporting.

Additionally, a formal and defined Technical Security Standards document (TSS-08 Standards for Vulnerability Management) has since been finalized. The capability has matured from previous years, prompting Audit Services to begin a regular continuous monitoring program of patch management activities, specifically.

These efforts are as approved in the Annual Audit Plan. This initial approach prioritizes critical systems to the organization's operations (see Statement of Scope below) with plans for future continuous monitoring efforts to iterate and expand the scope up the technology stack, including but not limited to: Applications, Middleware, Hardware, etc.

## Statement of Objectives

The objective of this continuous monitoring is to provide reasonable assurance to the Audit Committee on the effectiveness of ongoing security patch management activities. Specifically:

- To review and assess patching compliance for select s 15(1) servers.
- To determine if there are any unapplied critical security patches.

## Statement of Scope

The scope of this initial monitoring effort will focus on patching activities for the following s 15(1) servers critical to BCLC operations:

- s 15(1) and Casino s 15(1) servers s 15(1) .
- eGaming servers s 15(1) .

---

[1] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

## Statement of Methodology

The following procedures were conducted:

- Gathered and reviewed available reporting for patch management.
- Interviews and discussion with key stakeholders.
- Attendance and observation of Patch and Vulnerability Group (PVG) meetings.
- Reviewed patching processes and assessed activities against NIST (National Institute of Standards and Technology) best practices for effective patch and vulnerability management programs.

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes to key control areas during all engagements related to BCLC's core functions. Personnel changes can impact the control environment, effectiveness of key controls, and loss of risk and control knowledge. During this engagement, we discussed personnel changes, retirements, and revisions to roles with management. Audit Services noted no changes that had an impact on the control environment, effectiveness of key controls, and loss of risk and control knowledge.

## Audit Conclusions

Based on the audit work performed, we conclude that there are four (moderate) findings related to patch management requiring attention by Management (also see Appendix A):

1. Inventory.
2. Reporting KPI's and Metrics.
3. Follow-up and Remediation.
4. s 15(1)

Additionally, compliance for s 15(1) servers have averaged 75% and 83%, respectively, for the three-month period between November 2018 and January 2019. While s 15(1) servers are consistently almost fully compliant for the same period (99.5%).

# Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

# Audit Findings

Following are the most significant issues that we identified during our work along with associated recommendations to address these issues. To assist management in prioritizing action plans in response to our recommendations, we have categorized each issue by level of risk, using the following scale:

- High – Issue should be addressed and resolved immediately.

- Moderate – Issue requires management attention and should be addressed and resolved within a reasonable time period.

- Low – Issue is of lesser significance that is administrative in nature.  Any low risk findings have been discussed with management and therefore excluded from the report.

These rating levels are measured in the context of this audit and its objectives, rather than as related to overall corporate risk. Audit Services commits to conducting follow-up audits on all significant findings within 6 months from the date this audit report was issued.

## FINDING 1 INVENTORY (MODERATE)

**Finding**

The enterprise-wide tool utilized for IT inventory at BCLC is s 15(1) . Through interviews, Audit Services noted that not all teams rely upon s 15(1) as a central source of inventory information due to inaccuracies and data unreliability. Whether automated or manual, inventory management tools are the foundation for identifying and prioritizing all IT resources to monitor for vulnerabilities, threats, and patches. As a result, it makes it difficult and/or inefficient to achieve inventory accuracy and completeness during routine and/or emergency patching processes.

Risk:

Inaccurate or an incomplete inventory may result in unpatched servers, increasing the potential risk of a breach or attack.

**Recommendation**

Management should implement stronger controls and processes, included but not limited to, automated integration, to ensure new server builds and configurations are visible to patch management groups in a timely manner.

Implement stronger controls and processes to achieve accuracy, completeness, and efficient lifecycle maintenance (adding, changing, decommissioning) of IT assets within a centralized inventory data source.

**Management Response**

Management agrees with the finding and recommendation. BT has placed a strong focus on automation and process improvement across technology delivery teams, who will work with Service Management to drive ongoing improvements to our inventory accuracy. In addition, BT utilizes several other tools such as ^s 15(1) to complete systems deployment and patching. Further integrations between these tools and ^s 15(1) will be explored by September 30, 2019, and recommended changes from the analysis will be placed into the product backlog of teams and prioritized accordingly.

## FINDING 2 REPORTING KPI'S AND METRICS (MODERATE)

**Finding**

Per National Institute of Standards & Technology (NIST) recommendations, every organization should consistently measure their patch management program's effectiveness. Such measures will allow management to apply the appropriate corrective actions. At minimum, an effective program will include measures of 'susceptibility to attack' through (but not limited to) the number of patches, as well as, the number of vulnerabilities (in the context of the organization's unique security infrastructure and architecture).

Audit Services notes that current metrics capture the number of patched (compliant) servers to total servers. Reporting also captures 1) number of missing patches on non-compliant servers and 2) number of days of non-compliance. Current reporting does not capture the detailed Common Vulnerability Scoring System (CVSS) ratings, which can be used to determine the risk classification for the missing security patches on non-compliant servers.

Risk:

Existing metrics do not provide management with visibility into the risk classification levels for non-compliant servers.

**Recommendation**

Management should consider setting a target benchmark for patching compliance and consider enhancing reporting metrics by including the CVSS rating system for vulnerabilities on non-compliant servers, to help guide remediation efforts in compliance to BCLC Technical Security Standards.

**Management Response**

Management agrees with setting a patching compliance benchmark that will ensure risk is mitigated to an acceptable level. Currently BT is releasing all patches deemed "Important" and above per the CVSS system, and plans to include lower risk patches also as part of regular patching. Of those remaining, Management recommends escalating non-compliant systems to the appropriate owners and Management for resolution, to drive the necessary upgrades as quickly as possible. Target for achieving patching compliance benchmarks by September 30, 2019.

## FINDING 3 FOLLOW-UP AND REMEDIATION (MODERATE)

**Finding**

During post-deployment activities of the patching cycle, non-compliant servers and outstanding missing patches are not followed-up on and remediated in a timely manner. There is a presence of s 15(1)

Risk:

If non-compliant servers are not remediated in a timely manner, they are at risk of non-compliance to BCLC's Technical Security Standards.

**Recommendation**

Management should consider implementing processes that allow for a timely post-review of non-compliant servers for the purpose of identifying root cause and prioritizing remediation actions.

**Management Response**

Management agrees with this finding. Recent analysis of outstanding patches has revealed challenges with multiple-systems reboots being required during the patching cycle as the primary cause. We anticipate this issue will be resolved and eliminate most of the issue of outstanding patches. Per the findings noted above, improved reporting and escalation processes will ensure remaining systems are remediated. Target completion for reboot process improvement June 30, 2019.

## FINDING 4 s 15(1) (MODERATE)

**Finding**

Some servers are s 15(1)

Risk:

s 15(1)                                                                                    .

**Recommendation**

Management should consider s 15(1)

                                                                              .

**Management Response**

Management agrees with this finding and recommendation. This risk is tied to s 15(1)

# Appendix A – Summary of Ratings and Recommendations

| Theme/Area assessed<br>*adapted from NIST800-40v2 | Audit Services Rating | Recommendations |
|---|---|---|
| **1) INVENTORY** | 🟡 | Implement stronger controls and processes, included but not limited to, automated integration, to ensure new server builds and configurations are visible to patch management groups in a timely manner.<br><br>Implement stronger controls and processes to achieve accuracy, completeness, and efficient lifecycle maintenance (adding, changing, decommissioning) of IT assets within a centralized inventory data source. |
| **2) PVG (Patch and Vulnerability Group)** | 🟢 | n/a |
| **3) MONITORING** | 🟢 | n/a |
| **4) TESTING** | 🟢 | n/a |
| **5) TOOLS** | 🟢 | n/a |
| **6) FOLLOW-UP and REMEDIATION** | 🟡 | Implement processes that allow for a timely post-review of non-compliant servers for the purpose of identifying root cause and prioritizing remediation actions. |
| **7) TRAINING**<br>*(Note: The area of training was assessed in the context of teams responsible for patching, excluding vulnerability monitoring capability that resides with Cybersecurity)* | 🟢 | No issues, however, ensure that documentation is reviewed on a regular basis and revised as necessary. Ensure that new staff understand existing policies and procedures as it relates to change and patch management. Ensure that existing staff receive refresher training of policies and procedures. |
| **8) KPI's and METRICS** | 🟡 | Determine and set a target benchmark for patching compliance and consider enhancing reporting metrics by including the CVSS rating system for vulnerabilities on non-compliant servers, to help guide remediation efforts in compliance to BCLC Technical Security Standards. |
| **9) Other Observations:**<br>s 15(1) | 🟡 | s 15(1) |

# Return to Player Settings Audit – Q1 Billy Barker Casino Quesnel

Audit Services

June 7, 2019

bclc

# Table of Contents

# Transmittal Letter

June 27, 2019

Garth Pieper
Director, Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Pieper:

**Re:** **Return to Player (RTP) Audit – Initial Testing and Follow-up – Billy Barker Casino**

Attached is Audit Services' audit report on the RTP testing which occurred at Billy Barker Casino in Quesnel on February 20, 2019 with follow-up testing on June 6 and 7, 2019.

The scope of the engagement on February 20 was focused specifically on the RTP settings at Billy Barker Casino for a sample of slot machines. During the course of our work on February 20 at Billy Barker Casino, we noted that 4 of the 51 slot machines tested had their RTP settings set incorrectly. The technician fixed the RTP settings on February 20, 2019.

Based on these results, Audit Services made the decision to test 100% of RTP settings for the site with limited advanced notice to site staff (one business day). This test was completed over June 6 and 7, 2019. Audit Services noted that there was no error in all 121 slot machines tested.

We thank the management and staff of the Billy Barker Casino for their cooperation and assistance during this audit.

s 22

Sincerely

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc:     Kevin Sweeney, Director Security, Privacy and Compliance
        Tom Maryschak, Senior Manager Casino Operations
        Ken Bach, Regional Manager, Operations
        Lorenzo Paragallo, Manager, Business Operations

# Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

## Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at the Billy Barker Casino on all slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

## Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.  This engagement occurs annually.

## Statement of Methodology

Our methodology and approach included:

- Testing RTPs of all slot machines

- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)

- Interviews & inquiries

- Identifying process weaknesses, risks and controls

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Billy Barker Casino, BCLC staffing component consists of a Manager Business Operations and one Senior Technician. We noted during this audit, that the BCLC staff at Billy Barker Casinos had a minimal staff turnover rate.

## Conclusion

Audit Services found no RTP exceptions in the 121 machines tested on June 6 and 7, 2019.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

# Return to Player Settings Audit – Q1 Chances Dawson Creek

Audit Services

May 23, 2019

# Table of Contents

bclc

# Transmittal Letter

June 27, 2019

Garth Pieper
Director, Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Pieper:

**Re:     Return to Player (RTP) Audit – Chances Dawson Creek**

Attached is the Audit Services' report on the RTP testing which occurred at Chances Dawson Creek on May 23, 2019. The scope of our audit focused specifically on the RTP settings at Chances Dawson Creek for a selected sample of slot machines.

During the course of our work conducted at Chances Dawson Creek, we noted that all 75 machines tested had their RTP settings set correctly. In total, Chances Dawson Creek has 148 slot machines.

We thank the management and staff of Chances Dawson Creek for their cooperation and assistance during this audit.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc:     Kevin Sweeney, Director Security, Privacy and Compliance
        Tom Maryschak, Senior Manager Casino Operations
        Bal Bains, Regional Manager, Operations
        Cassandra McGarvie, Manager, Business Operations

## Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

## Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Chances Dawson Creek on randomly selected slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

## Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

## Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines

- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)

- Interviews & inquiries

- Identifying process weaknesses, risks and controls

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Chances Dawson Creek, BCLC staffing component consists of a Manager Business Operations and one Senior Technician. We noted during this audit, that the BCLC staff at Chances Dawson Creek has a minimal staff turnover rate.

## Conclusion

Audit Services found no RTP exceptions in the 75 machines tested on May 23, 2019.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

# Return to Player Settings Audit – Q1 Chances Fort St. John

Audit Services

May 23, 2019

bclc

# Table of Contents

bclc

# Transmittal Letter

June 27, 2019

Garth Pieper
Director, Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Pieper:

**Re:** **Return to Player (RTP) Audit – Chances Fort St. John**

Attached is the Audit Services' report on the RTP testing which occurred at Chances Fort St. John on May 23, 2019. The scope of our audit focused specifically on the RTP settings at Chances Fort St. John for a selected sample of slot machines.

During the course of our work conducted at Chances Fort St. John, we noted that all 75 machines tested had their RTP settings set correctly. In total, Chances Fort St. John has 149 slot machines.

We thank the management and staff of Chances Fort St. John for their cooperation and assistance during this audit.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc:     Kevin Sweeney, Director Security, Privacy and Compliance
        Tom Maryschak, Senior Manager Casino Operations
        Bal Bains, Regional Manager, Operations
        Lorenzo Paragallo, Manager, Business Operations

## Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

## Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Chances Fort St. John on randomly selected slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

## Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

## Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines

- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)

- Interviews & inquiries

- Identifying process weaknesses, risks and controls

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Chances Fort St. John, BCLC staffing component consists of one Senior Technician and a Manager Business Operations who is located at Prince George but travels to the Fort St. John site as needed. We noted during this audit, that the BCLC staff at Chances Fort St. John has a minimal staff turnover rate.

## Conclusion

Audit Services found no RTP exceptions in the 75 machines tested on May 23, 2019.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

# Return to Player Settings Audit – Q1 Playtime Kelowna

Audit Services

May 23, 2019

bclc

# Table of Contents

# Transmittal Letter

June 27, 2019

Garth Pieper
Director, Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Pieper:

**Re:** **Return to Player (RTP) Audit – Playtime Kelowna**

Attached is the Audit Services' report on the RTP testing which occurred at Playtime Kelowna on May 23, 2019. The scope of our audit focused specifically on the RTP settings at Playtime Kelowna for a selected sample of slot machines.

During the course of our work conducted at Playtime Kelowna, we noted that all 100 machines tested had their RTP settings set correctly. In total, Playtime Kelowna has 436 slot machines.

We thank the management and staff of Playtime Kelowna for their cooperation and assistance during this audit.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc:     Kevin Sweeney, Director Security, Privacy and Compliance
        Tom Maryschak, Senior Manager Casino Operations
        Brett Lawrence, Regional Manager, Operations
        Richard Frater, Manager, Business Operations

## Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

## Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Playtime Kelowna on randomly selected slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

## Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

## Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines

- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)

- Interviews & inquiries

- Identifying process weaknesses, risks and controls

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives.  We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Playtime Kelowna, BCLC staffing component consists of a Manager Business Operations, one Senior Technician and two Technicians. We noted during this audit, that the BCLC staff at Playtime Kelowna has a minimal staff turnover rate.

## Conclusion

Audit Services found no RTP exceptions in the 100 machines tested on May 23, 2019.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

# Encore Reward Points
## – Customer Support Centre
Audit Services


April 18, 2019

# Table of Contents

bclc

# Transmittal Letter

June 27, 2019

Martin Lampman
Director Customer Support Operations
74 West Seymour
Kamloops, BC V2C 1E2

Dear Jamie:

**Re:      Encore Reward Points – Customer Support Centre**

Attached is the Audit Services' report on Encore Reward Points – Customer Support Centre.

Our findings herein include three recommendations that address three moderate risk topics. Management has agreed with our recommendations and developed appropriate response plans to quickly address each item identified.

We thank the management and staff of the Customer Support Centre for their cooperation and assistance during this audit.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc:      Jamie Callahan, VP, Human Resources
         Brad Desmarais, VP, Casino and Community Gaming

# Introduction

This engagement was the next phase of the Token Review Engagement completed in FY2018. The Token Review engagement focused on tokens issued to PlayNow Player Account holders. This engagement, conducted in Q4 of FY2019 focused on tokens granted in the form of Encore rewards points to Encore Rewards Members. Encore Rewards is a loyalty program that allows members to earn and collect points for dining, playing table and slot games at Casinos, and to redeem points for freeplay. Members may also receive promotional freeplay. Our review covered a sample of transactions of Encore points issued by BCLC Customer Support Representatives (CSR) for the period between April 1, 2018 and February 28, 2019.

For the period reviewed, 30 CSR issued a total of 482,389 Encore Points to 114 different Encore Rewards card holders. The total dollar value of these points are approximately $2,500.

The Fraud Risk Assessment from 2018 identifies "Player Rewards Points" as an area of concern. The process of granting player loyalty points requires appropriate controls to mitigate risks of fraud and/or error, that if ineffective, could lead to potential negative impacts to corporate reputation and revenue.

# Statement of Objectives

The objective of this engagement was to assess the controls related to the process of granting Encore points by BCLC CSR to Encore Rewards Members. Specifically, to ensure that Encore points issued to patrons are:

- Authorized;
- Reasonable;
- Properly documented by the customer relationship platform (Salesforce) and;
- Issued in accordance to policy and/or Encore Rewards Program Terms & Conditions.

# Statement of Scope

The scope of this engagement included Encore points issued by BCLC CSR as a result of a complaint, dispute and/or inquiry initiated by the Encore Rewards Member, during the period of April 1, 2018 to February 28, 2019.

The scope excluded Encore points earned or issued by the Casino Service Providers and through various promotions and contests available to Encore Reward Members.

# Statement of Methodology

The following procedures were conducted:

- Interviews and inquiry with key personnel,
- Review of procedures and practices,
- Gather and analyze reporting of Encore Points issued by CSR and related Salesforce cases.

## Statement of Audit Standards

We conducted our audit in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes to key control areas during all engagements related to BCLC's core functions. Personnel changes can impact the control environment, effectiveness of key controls, and loss of risk and control knowledge. During this engagement, we discussed personnel changes with management. Audit Services noted moderate to high attrition which is generally typical for call centre operations.

## Audit Conclusions

Based on the audit work performed, we conclude that controls can be enhanced in the following three areas:

1. Policy and procedures documentation.
2. Authorization and Approval controls.
3. Segregation of Duties (SOD) controls.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services was given full access to all resources and information required to complete this review.

## Audit Findings

Following are the most significant issues that we identified during our work along with associated recommendations to address these issues. To assist management in prioritizing action plans in response to our recommendations, we have categorized each issue by level of risk, using the following scale:

- High – Issue should be addressed and resolved immediately.

- Moderate – Issue requires management attention and should be addressed and resolved within a reasonable time period.

- Low – Issue is of lesser significance that is administrative in nature. Any low risk findings have been discussed with management and therefore excluded from the report.

These rating levels are measured in the context of this audit and its objectives, rather than as related to overall corporate risk. Audit Services commits to conducting follow-up audits on all significant findings within 6 months from the date this audit report was issued.

## 1. POLICY AND PROCEDURES DOCUMENTATION (MODERATE)

### Finding

A policy as it relates to Customer Support-Issued Encore points does not exist. Additionally, the current procedural documentation in use includes multiple Knowledge Articles, maintained and available in the SalesForce Knowledge Article library for use by Customer Support Representatives (CSR). These articles capture varied scenarios and related procedures, however, contain conflicting thresholds and/or authorization/escalation instructions.

### Risk:

The absence of standard operational policy and unified procedures documentation containing a single approval matrix may lead to confusion and cause CSR to apply incorrect and/or inconsistent procedures, resulting in player dissatisfaction and/or frustration.

### Recommendation

Management should work with relevant stakeholders (including, but not limited to, Player Loyalty, Policy, and GMS Operations teams) to create and implement policy documentation for Customer Support-issued Encore Points. In addition, management should review existing procedures documentation for consistency; which may include streamlining existing related Knowledge Article procedures. Ensure CSR are aware and trained on updated documentation.

### Management Response

Management accepts this recommendation and will work with the appropriate teams to draft a policy and review procedure documentation for improvements.

## 2. AUTHORIZATION AND APPROVAL CONTROLS (MODERATE)

### Finding

Transactions in excess of documented thresholds are issued via multiple transactions. Direction to issue points is provided by Player Loyalty, however, approval is absent at the time of issue. Ineffective authorization and approval controls led to an error of issuing $200 worth of points in excess of the intended amount of $50.

### Risk:

Absence of oversight and control of large(r) points balances issued presents potential risk for abuse, fraud, and/or human error. It may also lead to inefficient processes and motivation to circumvent the control.

### Recommendation

Management should work with the GMS Operations team and Subject Matter Experts (SME) to align application controls with policy. In doing so, management should consider system capabilities and/or limitations and implement solutions that contain improved PrizeID controls and/or other stronger segregation of duties controls; particularly, to ensure approval and review activities, as a preventive control measure, are part of the control design.

**Management Response**

Management accepts this recommendation and will work with GMS Operations team on a solution; however, the solution may be hampered by limitations of system capabilities.

## 3. SEGREGATION OF DUTIES (SOD) CONTROLS (MODERATE)

**Finding**

Only one role type (and one set of related security permissions) is defined in the Casino Marketplace user matrix for all Consumer Services staff; there is no system approval workflow process.

Risk:

A lack of SOD controls presents opportunity for abuse and fraud.

**Recommendation**

In addition to recommendation 2 (above) management should also implement regular self-monitoring and review of Customer Support-Issued Encore points data for authorization, approval, and reasonability, as a detective control measure.

**Management Response**

Management accepts this recommendation, and as with the response for Recommendation 2, as long as the system capabilities allow for this. Management is at the initial stages of the reporting and review process.