Privacy Complaint Report of the Information and Privacy Commissioner (Ontario)

1. The proposed class members can be categorized into six types, based on their relationship with Casino Rama Resort ("Casino Rama"): patrons who are or were members of the Players' Passport Club rewards program ("PPC Members"), other patrons, past employees, current employees, vendors, and "self-excluders" (members of the Self-Exclusion Program administered by the Ontario Lottery and Gaming Corporation ("OLG")).

2. The Privacy Complaint Report (the "Report") of the Information and Privacy Commissioner of Ontario (the "IPC") addresses the duties owed under the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31 ("*FIPPA*" or the "*Act*") to patrons (including PPC Members) and self-excluders. For jurisdictional reasons described below, the Report does not address the duties owed to past and current employees or vendors. It is anticipated the Federal Privacy Commissioner may issue a report on privacy issues within federal jurisdiction, including duties owed under the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*").

3. IPC investigator Lucy Costa (the "Investigator") concluded that Casino Rama did not have reasonable security measures in place to prevent unauthorized access to records containing the Personal Information of self-excluders and Casino Rama patrons.[1]

---

[1] Summary, p. 1. "Personal Information" has the definition ascribed to it in the *FIPPA*, namely: recorded information about an identifiable individual, including,
(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
(c) any identifying number, symbol or other particular assigned to the individual,
(d) the address, telephone number, fingerprints or blood type of the individual,
(e) the personal opinions or views of the individual except where they relate to another individual,
(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
(g) the views or opinions of another individual about the individual, and
(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

4. The Investigator concluded that OLG could not confirm the amount or extent of information in possession of the hacker.[2]

5. There was a contract between OLG and the private sector company responsible for operating Casino Rama on behalf of OLG, CHC Casinos Canada Limited ("CHC" or the "Operator"). The Investigator concluded that OLG did not have reasonable contractual and oversight measures in place with CHC to ensure the privacy and security of the Personal Information of Casino Rama patrons and OLG self-excluders.[3]

6. Records of the patrons were in the custody of CHC but under the control of OLG.[4]

7. By October 27, 2016, a total of 39 Casino Rama network systems had been compromised during the cyberattack.[5]

8. On November 21, 2016, the hacker released 4.49 gigabytes of Casino Rama data on the internet. The release consisted of over 14,000 documents containing the information of approximately 10,990 individuals.[6]

Scope of the investigation

9. The Investigator was assigned by the IPC to investigate the circumstances of the privacy breach and, in particular, concerns regarding the adequacy of the safeguards in place at the time of the breach to ensure the security and confidentiality of records in the custody of CHC, but under the control of OLG, which is subject to *FIPPA*.[7]

10. At the inception of the investigation, the Investigator requested access to documentation and reports prepared by Casino Rama IT staff and by Mandiant (Casino Rama's cybersecurity

[2] Summary, p. 1.
[3] Summary, p. 1; para. 121.
[4] Para. 2.
[5] Para. 11.
[6] Para. 18.
[7] Para. 20.

expert retained by CHC's legal counsel in the aftermath of the breach). The Investigator was of the opinion that these documents were necessary to better understand the actions taken by the hackers to infiltrate the Casino Rama network, as well as the actions taken by Casino Rama in response to the breach, including the security measures in place at the time. OLG and CHC were, however, unwilling to grant access because of concerns that producing those documents might have the effect of waiving privilege over them within the context of another legal proceeding.[8]

11. The Investigator agreed that there could be potential legal repercussions and decided not to pursue access to the requested documents. CHC did offer to make portions of two reports available to the IPC for on-site examination, on the express basis that it was not waiving privilege over the reports by doing so. The first partial report was the executive summary of a forensic investigation into the breach; the second partial report was a list of recommended IT security measures and best practices for Casino Rama to implement. After reviewing the documents, the Investigator required additional information about the hacker and Casino Rama's actions in relation to the breach. Consequently, two further sets of representations from OLG and CHC were provided.[9]

12. The information at issue in the IPC investigation was related to three groups of individuals:[10]

- Casino Rama employees;
- Casino Rama patrons; and
- self-excluders.

13. The Investigator found that, while only information relating to Casino Rama employees and patrons was released online by the hacker, this data was stored on file servers that contained

[8] Para. 20.
[9] Paras. 21-23.
[10] Para. 26.

additional information relating to self-excluders. The Investigator found further that OLG and CHC have not been able to determine whether any additional information – beyond what was released online – was in fact stolen by the hacker, including information relating to self-excluders.[11]

14. The nature of the attack, however, was such that, if the hacker was able to steal one type of information from the compromised file servers, they would have been able to steal others. The types of security measures in place were the same for all the data stored on the compromised file servers.[12]

15. OLG and CHC confirmed that the data fields for the Personal Information of Casino Rama employees included:[13]

- name, mailing address, email address, telephone number;
- date of birth, social insurance number, driver's license number or other government issued identification numbers;
- performance reviews; and
- termination information.

16. For Casino Rama patrons, the data fields included:[14]

- name, mailing address, email address, telephone number;
- date of birth, social insurance number, driver's license number or other government issued identification numbers;
- signature;
- Casino Rama identifiers (*e.g.*, player number);

[11] Para. 28.
[12] *Ibid.*
[13] *Ibid.*
[14] Para. 29.

- gaming information (*e.g.*, average buy-in, wins and losses, gaming history);
- bank account numbers, credit application information, outstanding credit collection and information; and
- incident reports/complaints, including security, medical injury/mental health, intoxication/drug use, property/vehicle damage and exclusion of minors.

17. The information in the data fields relating to self-excluders consisted of Casino Rama audit files of the Self-Exclusion Program and included the following fields:[15]

- OLG subject ID;
- name, mailing address, date of birth;
- date of self-exclusion, place of self-exclusion;
- status;
- date of rescindment;
- place of rescindment; and
- comments.

18. The Investigator reviewed the above-described data fields and came to the conclusion that all of the information in them qualifies as "Personal Information" as defined in s. 2(1) of the *Act*.[16] This section of the *Act* defines the type of Personal Information which is considered to be sensitive, private information that requires organizations which collect the information to do so in compliance with the *Act*.

19. The Investigator was confronted with a legal issue with respect to her jurisdiction under the *Act*, on the basis of CHC's submission that all of the Personal Information was under the control of CHC, not OLG. CHC collected the information in the course of commercial activities

[15] Para. 30.
[16] Para. 31.

and was responsible for implementing security safeguards; CHC therefore argued that the relevant privacy statute is the federal *PIPEDA*.[17]

20. The Investigator agreed that the Personal Information of Casino Rama employees was under the control of CHC, which is not subject to the *Act.* The Investigator characterized CHC as the employer of all Casino Rama personnel. The Investigator's report therefore does not address statutory violations of the employees' Personal Information because that mandate falls within the federal legislation (*PIPEDA*) and the Office of the Privacy Commissioner of Canada. To date, a report has not been released by the Privacy Commissioner of Canada.[18]

21. With respect of the role of OLG, the Investigator found that all of the Personal Information for self-excluders and Casino Rama patrons was under the control of OLG and therefore subject to the rules and safeguards set out in the *Act*.[19]

The 2011 Interim Operating Agreement

22. As set out in the plaintiffs' certification record and statement of claim, there exists an Operating Agreement that was entered into between OLG, CHC, Casino Rama Services Inc. (a subsidiary of CHC which employs Casino Rama personnel) and CRC Holdings, Inc. (the U.S. corporation that owns CHC and is an affiliate of the defendant Penn International, which is domiciled in the U.S.) (the "Agreement"). The Agreement was produced to the Investigator although it has not been produced in these proceedings.[20]

23. The terms and conditions of the Agreement are summarized at paragraphs 44-47 of the Report (pages 11-13).The Investigator was particularly critical of the Agreement because there are no provisions specifically establishing or requiring measures to ensure the privacy and

[17] Para. 49.
[18] Para. 35.
[19] Para. 36.
[20] Para. 44

security of the Personal Information of self-excluders or Casino Rama patrons. The Agreement does not even mention the term "Personal Information", including in relation to Casino Rama's Customer Database.[21]

24. One of the many provisions of the Agreement which the Investigator found relevant to determining obligations under the *Act* was subsection 2.1(x): "The parties agree that the Customer Database is the property of OLG, that no-one else may use it without OLG's consent and that, among other obligations, the operator must keep the information confidential and secure, transfer all rights in the relation to the data base to OLG and on termination of the agreement, turn it over to OLG for OLG's exclusive use and continued development".[22]

25. The OLG attempted to rely on s. 2.1(x) as support that its privacy duties had been delegated to the Operator. The Investigator found, to the contrary, that s. 2.1(x) was designed primarily to protect OLG's commercial interests in Casino Rama patron data, and that the Agreement therefore did not provide adequate protections to ensure the privacy of Casino Rama patron data.[23]

26. At paragraphs 49-50 of the Report, the Investigator summarized one of the arguments advanced by OLG and CHC, being that, while the Customer Database was within the custody or control of OLG, "the Customer Database was not accessed in this cyberattack; it is not held on a windows-based system". The Investigator asked a series of follow-up questions regarding the alleged distinction between the Customer Database and the Casino Rama patron Personal Information that was accessed in the breach. In response to those questions, OLG and CHC acknowledged that the Customer Database is not the sole repository of Personal Information of Casino Rama patrons. Casino Rama creates and stores other documents containing patron

[21] Para. 122.
[22] Para. 6.4.
[23] Para. 128.

Personal Information, including but not limited to: documents related to Casino Rama lines of credit, security incident reports, and emails regarding customer service issues. Such documents do not form part of the Customer Database and are stored separately from it. Some of these documents were stored on the two compromised servers that were accessed in this cyberattack.[24]

27. Having stated that the Customer Database was not accessed in the cyberattack, OLG nevertheless argued that Personal Information that was accessed from the Customer Database was not under its control, pursuant to the Agreement. The Investigator disagreed, stating that "…OLG and CHC appear to rely on the separate treatment of the Customer Database in the Agreement to disavow OLG control over the patron data that was stolen. This is an untenable position…"[25]

Compliance with the *Act*

28. Commencing at paragraph 71 of the Report, the Investigator went on to assess whether Casino Rama complied with s. 4(1) of Regulation 460 of the *Act*, taking into account the nature of the records to be protected.

29. The Investigator characterized the records at issue in the investigation as electronic records of self-excluders and Casino Rama patrons which contained sensitive Personal Information of various types. One type was characterized as Personal Information that could be used to commit identity fraud against an individual, which is found in the records pertaining to Casino Rama patrons. Specifically, information consisting of: name, date of birth, address, social insurance number, driver's license number or other government-issued identification, signature, bank account number(s), and credit application information could be used by an identity thief to

[24] Paras. 50, 128.
[25] Para. 129.

steal an individual's identity and impersonate them to obtain false credit or other fraudulent benefits.[26]

30. The Investigator also characterized the Personal Information to be of a type that could lead to the embarrassment or stigmatization of individuals, referring both to the records pertaining to Casino Rama patrons and to the records pertaining to self-excluders: "A [Casino Rama] patron's outstanding credit collection information may contain details of their financial history that they would not want shared with others. Incident reports and complains about Casino Rama patrons may also contain sensitive information, including personal health information such as medical injuries or mental conditions. In addition, the very fact that an individual has registered for OLG's self-exclusion program could lead to their embarrassment or stigmatization. Any details or comments regarding incidents of identification and/or removal, would only add to the sensitivity of the records."[27]

31. With respect to the scope of the breach, the Investigator acknowledged at paragraph 76 of the Report that the Personal Information of approximately 10,990 individuals was released online, but that it is possible that the hacker stole additional records that has not been released online to date. CHC was not able to determine from its investigation which records had been stolen from the Casino Rama network as part of the attack. Casino Rama audit files containing the Personal Information of self-excluders were housed on the same file servers from which the hacker is known to have stolen Casino Rama data.

32. Commencing paragraph 78 on page 19, through to page 27, the Investigator reviewed how the hacker compromised Casino Rama systems, and what security measures were in place at the time of the breach, and considered whether those measures complied with s. 4(1) of

[26] Para. 74.
[27] Para. 75.

Regulation 460 of the *Act*. The Investigator concluded that there were a number of substantive security measures that were required by legislation to be in place, including the Alcohol and Gaming Commissioner of Ontario ("AGCO")'s *Registrar's Standards for Gaming*, and standards under s. 4(1) of Regulation 460 of the *Act*, which were not implemented.

33. The Investigator concluded that Casino Rama did not have reasonable measures in place to prevent unauthorized access to the Personal Information of self-excluders and Casino Rama patrons.[28]

34. The Investigator acknowledged the sophistication of the attack, including the tools and techniques used by the hacker to gain access to the Casino Rama network. She characterized the intruder as a motivated intruder with the skills and capacity to carry out a multi-staged attack. She characterized the hacker's technique of using emails targeting specific individuals as "spear phishing" that posed a "potentially high" threat.[29]

35. Nevertheless, the Investigator concluded that Casino Rama's response to the cyberattack, particularly the steps that it took early on in its response, did not amount to a timely and appropriate response to an incident of this nature. She found that, when a suspicious remote connection to an employee's work station revealed that the credentials of a Casino Rama IT staff member had been compromised, and that an unknown individual had full control over that employee's work station, there existed an alarming situation. Casino Rama's IT team and its assessment of the breach fell well below what constituted an adequate response at the initial steps it took after learning of the remote connection.

36. Further, as discussed at paragraph 106 of the Report, Casino Rama's IT team was wrong to believe that it had "resolved the issue" after taking certain initial steps. Specifically, without

[28] Para. 113.
[29] Paras. 96, 100.

an understanding of the nature of the remote connection, Casino Rama's IT team should have appreciated that the full size and scope of the attack remained unknown: "The problem could have been bigger than a single remote connection and in fact, we now know that it was."

37. The Investigator noted that:[30]

> further evidence of the low priority with which the incident was handled [was] demonstrated by the initial advice [Casino Rama] IT provided to the employee upon learning of the remote connection. The IT team logged the incident as 'called [IT staff member] and found out if he was remotely logged in to her computer, he said he wasn't, called [employee] back and let her know just to reboot the computer and to log in as herself.'
>
> …
>
> When investigating a security incident that is both alarming and of unknown scope, what is required at a minimum is a full diagnostic assessment of the affected system. Reviewing log files and analytics is an important part of this. It may also be useful to install new anti-virus software. However, equally important is identifying which other systems the affected computer may be communicating with and determining whether that communication is legitimate or not. In this context, a port scan or equivalent real-time analysis should be seen as a corresponding primary tool, not an after-effect precaution.

38. Based on her findings as summarized above, the Investigator concluded as follows:[31]

> I have concerns about the reasonableness of [Casino Rama] IT's investigation of the remote connection. To wait 8 days after initial detection of an incident that is both alarming and of unknown scope to conduct a full diagnostic assessment of the affected computer does not appear to a timely or appropriate response to an incident of this nature.

Audits leading up to the cyberattack

39. Commencing at paragraph 134 of the Report, the Investigator summarized the extent to which the OLG complied with its oversight measures. OLG asserted that it primarily relies on the AGCO to conduct regular inspections and periodic audits.[32]

40. In response to the Investigator requesting documents in support of regular inspections and audit reports, an AGCO audit report from 2015 was produced, including the most recent vulnerability assessment prior to the cyberattack – which was completed more than five years prior.[33]

---

[30] Paras. 108-09.
[31] Para. 112.
[32] Para. 134.
[33] Paras. 135-36.

41. The Investigator considered a five-year-old vulnerability assessment for an institution such as a casino to be too old and outdated for it to be considered an example of an adequate oversight measure within the context of the IPC's investigation.[34]

42. Having said that, the Investigator reviewed the audit results and recommendations. She was particularly critical because the audit report identified serious information security concerns, including a failure to adopt an industry standard/framework for IT management, with existing IT resources being utilized primarily to provide operational support. The auditors concluded:[35]

> Without a proper framework, the critical IT processes and controls required to meet business objectives and safeguard the integrity of the gaming systems and comply with regulatory requirements may be overlooked. For example, without adequate data protection controls, an organization may not meet regulatory requirements of *FIPPA*.

43. The auditors also recommended a data governance framework be created, because the audit revealed that Casino Rama's data protection, data retention, and data disposal measures and requirements were not defined or implemented.[36]

44. The auditors cautioned that, without a formal data governance framework, critical and sensitive data might not be adequately protected, resulting in data loss or breach. The auditors found that Casino Rama IT management was aware of the deficiency but did not take any measures due to limited IT resources.[37]

45. The response from Casino Rama management to the audit was to recommend that the findings of the auditors be removed from the audit report because the security recommendations were based on new AGCO *Registrar's Standards for Gaming* which had not yet been implemented. The Investigator characterised the Casino Rama response to the audit as follows:[38]

---

[34] Para. 136.
[35] Para. 137.
[36] *Ibid.*
[37] *Ibid.*
[38] Para. 140.

> I find this to be a remarkable comment. The AGCO Audit Report specifically notes control deficiencies that put [Casino Rama] at risk of not only not meeting regulatory requirements of *FIPPA* but potentially resulting in a data breach and, in response to this, [Casino Rama]'s position is that these findings 'are not a compliance concern'.

46. The Investigator found that the failure of OLG and Casino Rama to implement the audit report recommendations contributed to the cyberattack:[39]

> If a data governance framework had been in place prior to the cyberattack, Casino Rama would have been in a position to conduct a threat risk assessment to assess the adequacy of the security measures in place to protect Personal Information of [self-excluders and Casino Rama patrons] given its sensitivity, level of risk and the types of threats posed to it.

[39] Para. 145.