Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PR16-40

Ontario Lottery and Gaming Corporation

January 30, 2019

Summary: On November 9, 2016, the Ontario Lottery and Gaming Corporation (OLG) notified the Office of the Information and Privacy Commissioner/Ontario (the IPC) of a possible privacy breach under the *Freedom of Information and Protection of Privacy Act* (*FIPPA* or the *Act*). OLG advised that a hacker had managed to steal information about employees and patrons of Casino Rama Resort (CRR) and was threatening to make the information public unless he was paid a ransom. OLG could not confirm the amount or extent of information in possession of the hacker. OLG further stated that the hacker claimed to have 154 gigabytes of CRR data and had posted examples of the information online. On November 21, 2016, the hacker released 4.49 gigabytes of CRR data on the Internet reported to consist of more than 14,000 documents.

In this report, I conclude that CRR did not have reasonable security measures in place to prevent unauthorized access to records of personal information of CRR patrons and individuals registered for OLG's self-exclusion program (OLG self-exclusion registrants); however, since the breach, CRR has taken steps to address the gaps in its systems and processes. Although I am generally satisfied with CRR's response to the breach in this regard, this report makes additional recommendations to address some specific shortcomings.

The other pillar of the IPC's investigation concerns the contract between OLG and the private-sector company responsible for operating CRR on behalf of OLG, CHC Casinos Canada Limited (CHC or the Operator). In this report, I conclude that OLG did not have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants. This report also makes recommendations to address these shortcomings.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*; R.R.O. 1990, Regulation 460; *Criminal Code*; *Ontario Lottery and Gaming Corporation Act*; *Gaming Control Act*; *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Orders and Investigation Reports Considered: Order P-404; Order PO-3520; Privacy Investigation Report PC12-39.

Cases Considered: *Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner)*, [1999] O.J. No. 4072 (C.A.); *Canada (Information Commissioner) v. Canada (Minister of National Defence)* 2011 SCC 25, [2011] 2 SCR 306.

BACKGROUND:

[1] On November 9, 2016, the Ontario Lottery and Gaming Corporation (OLG) notified the Office of the Information and Privacy Commissioner/Ontario (the IPC) of a possible privacy breach under the *Freedom of Information and Protection of Privacy Act* (*FIPPA* or the *Act*). OLG advised that a hacker had managed to steal information about employees and patrons of Casino Rama Resort (CRR) and was threatening to make the information public unless he was paid a ransom. OLG could not confirm the amount or extent of information in possession of the hacker. OLG further stated that the hacker claimed to have 154 gigabytes[1] of CRR data and had posted examples of the information online. On November 21, 2016, the hacker released 4.49 gigabytes of CRR data on the Internet reported to consist of more than 14,000 documents.

[2] At the time of the cyberattack, the day-to-day operations of CRR were carried out on behalf of OLG by a private-sector company, CHC Casinos Canada Limited (CHC or the Operator). After further correspondence with OLG and CHC, the IPC decided to investigate the circumstances of the privacy breach and, in particular, concerns regarding the adequacy of the safeguards in place at the time to ensure the security and confidentiality of records in the custody of CHC but under the control of OLG.

[3] On October 14, 2016, a phishing email was sent to 11 CRR employees purporting to be from a CRR manager. The pretense of the email was to inform employees of a change to the CRR work schedule for the upcoming holidays. The email contained a link to what it claimed was a chart with information about an updated work schedule. What the link actually pointed to, however, was malware hosted on a server with a Russian Internet Protocol (IP) address.

[4] At the time of this incident, CRR had email security installed to scan the content of inbound email messages and their attachments for spam and malware, but the

[1] A gigabyte is a common unit of measurement for digital storage space. In his ransom emails, the hacker uses conflicting terms to describe the amount of CRR data he purports to have stolen. Sometimes he claims to have stolen 154 "Gigs," which is the shortened, colloquial form of "gigabyte." Other times, however, he states 154 "Gigabits," which is a smaller unit of measurement (equal to 1/8th the size of a gigabyte) more commonly used to specify digital network speeds. Following OLG's submissions, I have opted to describe the amount of CRR data purportedly stolen by the hacker as 154 gigabytes.

program failed to recognize and filter out the phishing email as malicious.

[5] While some of the CRR employees who received the phishing email recognized it as suspicious and deleted it, others did not and clicked on the malicious link embedded in it. This resulted in a multi-stage malware program being executed and saved on their workstations.

[6] CRR also had firewalls deployed to protect its network, but these did not prevent the malware from being downloaded to the employee's workstations. In addition, CRR had antivirus and antimalware software installed on the affected employees' workstations, but the software failed to detect the programs executed and saved on the workstations as malware.

[7] On the same day, October 14, 2016, at least one of the recipients of the phishing email contacted the CRR manager from whom the phishing email purported to be to report that they were unable to open the link to the modified work schedule in his email. (When clicked, the malicious link did not display anything on the user's computer screen; to the user, it appeared to be a non-functioning hyperlink.) In response, the CRR manager sent an email to all other CRR managers, including those in the information technology department (Casino Rama IT), advising them that they may have received a "spam" email from what appears to be his account and directing them to avoid clicking on the link inside it. No investigation was commenced by Casino Rama IT into the phishing email.

[8] On October 19, 2016, an employee who had also received the phishing email was prevented from logging in to her workstation because another user was already logged in to it remotely. The employee reported this event to Casino Rama IT. The user account that was logged in remotely to the employee's workstation belonged to a Casino Rama IT staff member. Casino Rama IT determined that the particular staff member was not responsible for the remote connection and began an investigation into this incident.

[9] During their investigation Casino Rama IT found that Dropbox had been installed on the employee's workstation; however, they determined that no data had been uploaded to Dropbox as access to the service from the employee's workstation was already blocked by CRR's firewall. They also analyzed security log files and installed new antivirus software on the employee's workstation, but were unable to determine the source of the remote connection.

[10] On October 19 and 20, 2016, Casino Rama IT blocked access to Dropbox from all computers on the CRR network and disabled the remote desktop program. On October 21, 2016, administrator, exchange server, firewall and router passwords were changed.

[11] Casino Rama IT believed that the steps taken above had resolved the issue of the remote connection on the employee's workstation; however, on October 27, 2016, they decided to conduct a port scan of the employee's workstation. The port scan

identified a Russian IP address attempting to communicate with the employee's workstation. Casino Rama IT immediately blocked communication with that IP address using CRR's firewall. The IP address communicating with the employee's computer was the same as the one pointed to by the malicious link in the phishing email. After the IP address was blocked, the hacker did not have any means of access to the CRR network. However, by this time, a total of 39 CRR systems had been compromised during the cyber attack.

[12] On November 4, 2016, CRR became aware of an email from the hacker in which he claimed to have 154 gigabytes of CRR data. The email attached links to a website with sample files of confidential CRR data to demonstrate that CRR data had been stolen. The email included a ransom demand and a threat to start releasing data to the public in the event that the ransom was not paid within seven days.

[13] On the same day, November 4, 2016, CHC provided notice of the breach to OLG, the Alcohol and Gaming Commission of Ontario and the Ontario Provincial Police. CHC also began an investigation into whether any active threat actor remained in the environment.

[14] On November 8, 2016, CRR received a further email from the hacker indicating that if payment were not received in three days or less, there would be a "data dump."

[15] On November 9, 2016, OLG and CHC provided notice of the breach to the IPC. The Office of the Privacy Commissioner of Canada and the Royal Canadian Mounted Police were also notified.

[16] On November 10, 2016, OLG publicly announced that CRR had been the subject of a data breach. On the same day, OLG and CHC began the process of offering credit monitoring to all current employees, former employees and patrons who were determined to be eligible for credit monitoring.

[17] On November 11, 2016, the hacker posted links to two websites with sample files of confidential CRR data. In the message accompanying the links, the hacker stated that in 72 hours the first data dump would be made available on the Internet. On this same day OLG and CHC sent takedown notices to the websites where sample files of confidential CRR data had been posted, and the files were subsequently removed.

[18] On November 21, 2016, the hacker released 4.49 gigabytes of CRR data on the Internet. The release is reported to consist of over 14,000 documents containing the information of approximately 10,990 individuals.

INVESTIGATION:

[19] After receiving notification of the privacy breach, the IPC requested additional

information from OLG and CHC. The IPC received a response from OLG and CHC in a letter dated January 20, 2017. This matter was then assigned to me as the investigator.

[20] During my investigation, I requested three sets of representations from OLG and received joint responses from OLG and CHC. I received the first set of representations in two installments on June 28 and August 9, 2017, respectively. One of the issues that arose at this point of the investigation was whether the *Act* provides a sufficient statutory framework to ensure that documents produced or supplied in the course of a privacy complaint investigation by the IPC are granted legal privilege as if the investigation were a proceeding in court. At issue were the documentation and reports produced by Casino Rama IT and cybersecurity experts retained by CHC's legal counsel in the aftermath of the breach. I requested copies of these documents to better understand the actions taken by the hacker to infiltrate the CRR network as well as the actions taken by CRR in response to the breach, including the security measures in place at the time. However, OLG and CHC were unwilling to grant access due to concerns that producing these documents may have the effect of waiving privilege over them within the context of another legal proceeding.

[21] I agreed with OLG and CHC's assessment of the potential legal repercussions and decided not to pursue access to the documents. While the *Act* provides legal protections for documents produced or supplied in the course of an "inquiry" respecting an appeal of an access to information request, it does not provide similar protections in the case of privacy complaint investigations. As noted in IPC Order P-404,

> A compliance investigation undertaken by the office of the Information and Privacy Commissioner/Ontario is not an inquiry for the purposes of the *Act*, and records which are produced in the course of a compliance investigation are not records produced in the course of an inquiry pursuant to section 52(1). Accordingly, the privilege described in section 52(9) does not extend to the records at issue in this appeal [i.e., records produced in the course of a privacy complaint investigation].

[22] CHC did offer to make available for on-site examination portions of two reports to the IPC 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 was a list of recommended IT security measures and best practices for CRR to implement. I viewed these documents on September 11, 2017.

[23] After reviewing the documents, I still required additional information about the hacker's and CRR's actions in relation to the breach. I received two further sets of representations from OLG and CHC on November 17, 2017, and March 2, 2018.

ISSUES:

[24] I identified the following issues as arising from this investigation:

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

2. Does the *Act* apply to the information at issue?

3. Did CRR have reasonable security measures in place to prevent unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with section 4(1) of Regulation 460 of the *Act*?

4. Did OLG have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with the requirements of the *Act* and its regulations?

DISCUSSION:

Issue 1: Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

[25] Section 2(1) of the *Act* states in part:

> "personal information" means 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,
> >
> > . . .
> >
> > 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;

[26] The information at issue in this investigation relates to three groups of individuals:

- CRR employees;
- CRR patrons; and
- individuals registered for OLG's self-exclusion program (OLG self- exclusion registrants).

[27] While only information relating to CRR employees and CRR patrons was released online by the hacker, this data was stored on fileservers that contained additional information relating to OLG self-exclusion registrants. 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 OLG self-exclusion registrants. However, the nature of the attack was such that if the hacker was able to steal one type of information from the compromised fileservers, he 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 fileservers.

[28] OLG and CHC confirmed the data fields for the information relating to each of the three groups of individuals. The information relating to CRR employees included the following:

- Name, mailing address, email address, telephone number;
- Date of birth, social insurance number, driver's license number or other government issued identification number;
- Performance reviews; and
- Termination information.

[29] The information relating to CRR patrons included the following:

- Name, mailing address, email address, telephone number;
- Date of birth, social insurance number, driver's license number or other government issued identification number;
- Signatures;
- Casino Rama identifiers (e.g., player number);

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

[30] The information relating to OLG self-exclusion registrants consisted of CRR audit files of the self-exclusion program. It included the following fields:

- 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.

[31] Based on the above, I find that the information at issue qualifies as "personal information" as defined in section 2(1) of the *Act*. The information relating to CRR employees meets the requirements of paragraphs (a), (b), (c), (d) and (g) of the definition; the information relating to CRR patrons meets the requirements of paragraphs (a), (b), (c), (d), (g) and (h); and the information relating to OLG self-exclusion registrants meets the requirements of (a), (c), (d), (g) and (h).

Issue 2: Does the Act apply to the information at issue?

[32] Section 69(1) of the *Act* states:

> This Act applies to any record in the custody or under the control of an institution regardless of whether it was recorded before or after this Act comes into force.

[33] Although I have found that the sets of information relating to CRR employees, CRR patrons and OLG self-exclusion registrants qualify as "personal information" as defined in section 2(1) of the *Act*, this by itself does not mean that the rules and safeguards set out in the *Act* apply to them. Whether the *Act* applies to any of these sets of personal information depends on whether each was "in the custody or under the control" of OLG at the time of the incident. I will now turn to this question.

[34] OLG and CHC submit that neither the personal information of CRR employees nor the personal information of CRR patrons that was accessed in the attack, nor the IT systems and accounts that were compromised in the attack, including the personal information of OLG self-exclusion registrants, were under the control of OLG at the material times. Rather, they submit that this information was under the control of CHC, which collected the information in the course of commercial activities and was responsible for implementing security safeguards. OLG and CHC submit that CHC is subject to, and has complied with, the federal *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.

[35] I agree with OLG and CHC's claim that the personal information of CRR employees was under the control of CHC and was not subject to the *Act*. As set out below, CHC was the employer of all CRR personnel. This information is not at issue in this investigation.

[36] However, I disagree with OLG and CHC's position with respect to the personal information of CRR patrons and OLG self-exclusion registrants. For the reasons set out below, I find that the personal information of CRR patrons and OLG self-exclusion registrants that was accessed in the attack was under the control of OLG and therefore subject to the rules and safeguards set out in the *Act*.

The statutory and regulatory regime governing OLG and the operation of CRR

[37] Before setting out the reasons for my finding, it is important to understand the statutory and regulatory regime governing OLG with respect to the operation of casinos and other gaming activities. The role and responsibilities of OLG are established by statute and described in other documents, as set out below.

[38] The conduct and management of lottery and gaming activities by the province is authorized pursuant to s. 207(1)(a) of the *Criminal Code,* 1985, as follows:

> 207 (1) Notwithstanding any of the provisions of this Part relating to gaming and betting, it is lawful
>
> > (a) for the government of a province, either alone or in conjunction with the government of another province, to conduct and manage a lottery scheme in that province, or in that and the other province, in accordance with any law enacted by the legislature of that province; . . .

[39] Further to this authorization, OLG is established as a corporation under section 2 of the *Ontario Lottery and Gaming Corporation Act*, 1999 (*OLGCA*) with the following objects set out at section 3 (in part):

> 1. To develop, undertake, organize, conduct and manage lottery schemes on behalf of Her Majesty in right of Ontario.

> 2. To provide for the operation of gaming sites.
>
> 3. To ensure that lottery schemes and gaming sites are conducted, managed and operated in accordance with the Criminal Code (Canada), this Act and the Gaming Control Act, 1992 and the regulations made under them.
>
> 4. To provide for the operation of any business that the Corporation considers to be reasonably related to operating a gaming site or lottery scheme, including any business that offers goods and services to persons who play lottery schemes in a gaming site.
>
> . . .

[40] In addition, under the *Gaming Control Act*, 1992, the Registrar of Alcohol, Gaming and Racing is authorized to establish standards and requirements to regulate the conduct, management and operation of lottery schemes and gaming sites in Ontario. The *Registrar's Standards for Gaming* (the Gaming Standards) apply to OLG and all operators of gaming sites in Ontario. The Gaming Standards address issues of data governance with respect to player personal information as follows (in part):

> 1.37 **Player information shall be securely protected and its usage controlled by OLG.**
>
> **Requirements** – At a minimum:
>
> 1. Data collection and protection requirements for player personal information shall meet those set out in the Freedom of Information and Protection of Privacy Act.
>
> 2. Player information shall only be used for OLG's business unless there is prior approval from OLG.

[41] The Gaming Standards also address issues of responsible gambling with respect to OLG's self-exclusion program as follows (in part):

> 2.6 **OLG shall provide a common voluntary self-exclusion program.**
>
> **Requirements** – At a minimum:
>
> . . .
>
> 5. Operators shall take active steps to identify, and if required, remove self-excluded persons when they are found to be in breach of their self-exclusion agreement.

[42] OLG is accountable to a responsible minister designated by the Lieutenant Governor in Council to administer the *OLGCA*, who historically has been the Minister of Finance. The accountability relationship between OLG and the Ontario government is supplemented by a 2011 *Memorandum of Understanding between the Minister of Finance and the Ontario Lottery And Gaming Corporation* (MOU) which, among other provisions, sets out OLG's information management responsibilities, including in relation to the purchase of services, as follows (in part):

> 8.3 The Corporation acknowledges that it is subject to FIPPA and the Corporation shall respond to access requests and privacy investigations and fulfill all requirements of FIPPA.
>
> . . .
>
> 8.7 With respect to the management of recorded information the Corporation will:
>
> > (a) ensure that managers follow appropriately defined processes of retention and disposal consistent with the directives and Legislation set out in Schedules A and B hereto;
> >
> > (b) ensure that managers and staff create full, accurate and reliable records that document and support significant business transactions, decisions, events, policies and programs;
> >
> > (c) hold managers accountable for managing the recorded information that is under their custody and control;
>
> 8.8 The Corporation acknowledges that property and/or services ordered/purchased by the Corporation are purchased by the Corporation for the use of the Crown in Right of Ontario.[2]

[43] OLG's Annual Reports for the fiscal years 2014-2015, 2015-2016 and 2016-2017 describe its ownership and management of CRR and other casinos, as well as their operation by private sector companies under operating agreements for each casino:

> **OLG Resort Casinos**
>
> OLG is responsible for conducting and managing gaming at four Resort Casinos – Caesars Windsor, Casino Rama, Casino Niagara and Niagara Fallsview Casino Resort. These sites are operated, under contract, by private operating companies.

---

[2] See https://about.olg.ca/wp-content/uploads/sites/28/2016/08/memo_understanding_EN.pdf.

. . .

C1. Resort Casinos revenue

OLG is responsible for four Resort Casinos – Caesars Windsor, Casino Rama, Casino Niagara and Niagara Fallsview Casino Resort ("Fallsview"). These sites are owned and managed by OLG with day-to-day operations carried out by private sector operators pursuant to the terms of their respective operating agreements. The private sector operator is the employer for all employees of each Resort Casino.[3]

[44] The contractual relationship between OLG and CHC is set out in a 2011 Interim Operating Agreement (the Agreement) entered into between OLG, CHC (referred to in the Agreement as the "Operator"), Casino Rama Services Inc. (a subsidiary of CHC which employs CRR personnel), and CRC Holdings, Inc. (the U.S. corporation that owns CHC). This Agreement, which replaces an earlier original development agreement (the DOA), was to continue in effect until a new operator was retained by OLG. However, the Agreement remained in effect at the time of the incident.

[45] The opening statements to the Agreement acknowledge that OLG has the statutory authority to conduct and manage casino gaming and to provide for the operation of casinos in Ontario.

[46] Relevant terms in the Agreement are defined, as follows (in part):

"Casino" means those areas in the Complex which are intended to be used, or are used, for the purpose of playing or operating a Game of Chance, together with all support facilities related to gambling;

"Complex" means the Complex Lands and all Improvements thereon, including the Casino, the Hotel, the Entertainment Centre, the surface Parking and any future developments . . .

"Complex Assets" means all personal property and other assets used or held for use in connection with the operation of the Complex, wheresoever situate, whether owned by OLG as of the date hereof or acquired from and after the date hereof by OLG or by the Operator using funds from the Bank Accounts or otherwise for the account and expense of the Complex, including the Approved Operating Policies;

"Customer Database" means the customer database for the Complex that was originally developed by the Operator pursuant to the Original DOA,

---

[3] OLG's annual reports are available at https://about.olg.ca/financial-annual-reports/.

> which the Operator continues to develop and maintain pursuant to the Original DOA as of the date hereof, as such database may be further developed by the Operator during the remainder of the Original Term in accordance with the Original DOA and during the Interim Operating Period in accordance with this Agreement;

[47] Several provisions of the Agreement relevant to the issues raised in this report are summarized here (numbers in parenthesis refer to articles of the Agreement):

> (i) The parties agree that the Province of Ontario must conduct all Games of Chance carried on at the Complex as required under s. 207(1)(a) of the *Criminal Code*. (2.2(a))
>
> (ii) OLG acknowledges its obligation to conduct and manage Games of Chance in the Casino and agrees that it is obliged to cause the Casino to be operated for the purposes of gaming for the duration of the Agreement (2.1(b), 2.16)
>
> (iii) OLG "retains and appoints the Operator as an independent contractor . . . to operate the Complex" and "retains and appoints the Operator as OLG's sole and exclusive agent to operate on behalf of and for the account of OLG the Games of Chances and all other activities related thereto to be carried on in the Casino." The Operator accepts these appointments. (2.1)
>
> (iv) The Operator agrees to operate the Casino in compliance with OLG's obligations under s. 207(1)(a) of the *Criminal Code*. (2.2)
>
> (v) The Operator agrees to comply with OLG Approved Operating Policies and to provide OLG with working space and access to all areas of the Casino. (2.2)
>
> (vi) The Operator agrees to perform various services in relation to the Casino Complex, including (2.3):
>
> > . . .
> >
> > (b) do or cause to be done all things relating to the Operation of the Complex which are necessary to ensure compliance with Applicable Law;
> >
> > (c) perform and, where desirable, contract for all things necessary or advisable for the proper, efficient and secure operation of the Complex;
> >
> > . . .

(k) protect, perfect and enforce rights relating to the Complex, and pursue claims against third parties relating to the Complex; and

(l) perform such other actions as it may, acting reasonably, consider necessary or advisable to carry out the intent of this Agreement.

(vii) The Operator agrees to adopt and use Approved Operating Policies for gaming and non-gaming activities and continue to develop these in cooperation with and subject to the approval of OLG. (2.4)

(viii) The Operator is obliged to keep books of account and other records necessary to reflect the operation of the Complex, to prepare reports for OLG and to make available to OLG for inspection all reports, accounts, records and other documents relating to the operation of the Complex. (4.7, 4.11)

(ix) The Operator agrees that all intellectual property, including all data bases, developed for use in conjunction with the Complex and all software developed or acquired by the Operator as an expense of the Complex, for use in connection with the Casino, and in which the Operator owns copyright, is the property of OLG. (6.2, 6.3)

(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 Database to OLG and, on termination of the Agreement, turn it over to OLG for OLG's exclusive use and continued development. (6.4)

(xi) In the event of a prospective transfer to a New Operator in a competition process, the Operator agrees to cooperate with OLG by providing any information, documents and other materials comprising Complex Assets, subject to certain exclusions and conditions, including confidentiality and non-disclosure agreements. (7.1)

(xii) On termination of the Agreement, the Operator agrees to turn over possession and control of all Complex Assets to OLG or its designate, including all original records, documents and books of account (8.6).

(xiii) Other provisions confirm that all Complex Assets are the sole and exclusive property of OLG. (10.2)

(xiv) Enforcement provisions contemplate the non-binding mediation of disputes, but entitle the parties to seek resolution of disputes in

> accordance with normal remedies available at law, with the option of arbitration. (11.1, 11.2)

Is the personal information of CRR patrons and OLG self-exclusion registrants in the custody or control of OLG?

[48] OLG and CHC submitted the following arguments and information in support of their claim that neither the personal information of CRR patrons that was accessed in the attack nor the IT systems nor accounts that were compromised in the attack, including the personal information of OLG self-exclusion registrants, were under the control of OLG at the material times.

[49] In answer to questions regarding the application of *FIPPA*, OLG and CHC submitted:

> OLG and CHC agree that OLG is an institution subject to *FIPPA* and that personal information that is within OLG custody or its "control" is within the purview of *FIPPA*.
>
> *Customer Database:* OLG and CHC agree that the Customer Database is within the purview of FIPPA as it is within OLG's control. Pursuant to s. 6.4 of the Interim Operating Agreement, the Customer Database is the property of OLG and any third party access to the same requires OLG's written approval. Further, pursuant to s. 2.1 (b) of the Interim Operating Agreement, OLG has retained CHC as its sole and exclusive agent for the purpose of operating lottery schemes on behalf of OLG at Casino Rama. The collection, use and retention of personal information of Casino Rama customers, as reflected in the Customer Database, is within the scope of the Operator's authority as OLG's agent for the purposes of operating lottery schemes. However, the Customer Database was not accessed in this cyberattack; it is not held on a Windows-based system.
>
> *Employee Personal Information:* OLG and CHC agree that the personal information of Casino Rama employees is not within the purview of *FIPPA* as it is not within OLG's control. Section 2.9 of the Interim Operating Agreement expressly provides for the Operator to establish CSRI as a CHC subsidiary to act as the employer for all personnel working at the facility. CSRI employees are not employees of OLG. They do not form part of OLG's head count, are not subject to the *Public Service of Ontario Act,* and are not eligible for membership in the Ontario Public Service Pension Plan. CSRI, not OLG, controls personal information relating to Casino Rama's workforce, which thus does not fall within the purview of *FIPPA*.
>
> Question 20 As noted above in the response to Question 19, the Customer Database is within OLG's control and is thus subject to *FIPPA*. As such, it is managed in accordance with *FIPPA* requirements. Personal information

> at Casino Rama that is not within OLG's control is not subject to *FIPPA*. This information, including the personal information of Casino Rama employees, is managed by CHC, consistent with its obligations as an organization subject to [*Personal Information Protection and Electronic Documents Act*].

[50] In answer to a series of follow-up questions regarding the distinction between the customer database and the personal information that was accessed in the attack, OLG and CHC submitted:

> [T]he Customer Database is not the sole repository of personal information of Casino Rama patrons. In the ordinary and necessary course of business, Casino Rama creates and stores other documents containing patron 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 servers that were accessed in the cyberattack. . . .
>
> The personal information accessed in the cyberattack was stored on two Windows servers [] that house network folders in which Casino Rama employee documents are stored. The Customer Database is stored on an entirely different, non-Windows server. . . .
>
> We do not agree that the personal information of patrons that was accessed in the attack, or the IT systems or accounts that were compromised, were under the control of OLG at the time of the cyberattack, although OLG and the AGCO had a right of access to certain of the same personal information (as is often the case in regulated industries). The federal Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) also had a right of access to certain of the same personal information.

(i) Factors relevant to determining "custody or control"

[51] The IPC has developed a series of questions to assist in the determination of whether records are in the custody or under the control of an institution and thus subject to *FIPPA*. The following passage from Order PO-3520 outlines the IPC's historical approach to this issue:

> This office has developed a list of factors to consider in determining whether or not a record is in the custody or control of an institution, as follows. The list is not intended to be exhaustive. Some of the listed factors may not apply in a specific case, while other unlisted factors may apply.

- Was the record created by an officer or employee of the institution?

- What use did the creator intend to make of the record?

- Does the institution have a statutory power or duty to carry out the activity that resulted in the creation of the record?

- Is the activity in question a "core", "central" or "basic" function of the institution?

- Does the content of the record relate to the institution's mandate and functions?

- Does the institution have physical possession of the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement?

- If the institution does have possession of the record, is it more than "bare possession"?

- If the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purposes of his or her duties as an officer or employee?

- Does the institution have a right to possession of the record?

- Does the institution have the authority to regulate the record's content, use and disposal?

- Are there any limits on the use to which the institution may put the record, what are those limits, and why do they apply to the record?

- To what extent has the institution relied upon the record?

- How closely is the record integrated with other records held by the institution?

- What is the customary practice of the institution and institutions similar to the institution in relation to possession or control of records of this nature, in similar circumstances?

[52] The following factors may apply where an individual or organization other than the institution holds the record:

- If the record is not in the physical possession of the institution, who has possession of the record, and why?

- Is the individual, agency or group who or which has physical possession of the record an "institution" for the purposes of the *Act*?

- Who owns the record?

- Who paid for the creation of the record?

- What are the circumstances surrounding the creation, use and retention of the record?

- Are there any provisions in any contracts between the institution and the individual who created the record in relation to the activity that resulted in the creation of the record, which expressly or by implication give the institution the right to possess or otherwise control the record?

- Was there an understanding or agreement between the institution, the individual who created the record or any other party that the record was not to be disclosed to the institution?[4] If so, what were the precise undertakings of confidentiality given by the individual who created the record, to whom were they given, when, why and in what form?

- Is there any other contract, practice, procedure or circumstance that affects the control, retention or disposal of the record by the institution?

- Was the individual who created the record an agent of the institution for the purposes of the activity in question? If so, what was the scope of that agency, and did it carry with it a right of the institution to possess or otherwise control the records? Did the agent have the authority to bind the institution?

- What is the customary practice of the individual who created the record and others in a similar trade, calling or profession in relation to possession or control of records of this nature, in similar circumstances?

- To what extent, if any, should the fact that the individual or organization that created the record has refused to provide the institution with a copy of the record determine the control issue?

[53] In determining whether records are in the "custody or control" of an institution, the above factors must be considered contextually in light of the purpose of the legislation.

[54] In *Canada (Information Commissioner) v. Canada (Minister of National Defence)*,

---

[4] Orders M-165 and MO-2586.

the Supreme Court of Canada adopted the following two-part test on the question of whether an institution has control of records that are not in its physical possession:

> (1) Do the contents of the document relate to a departmental matter?
>
> (2) Could the government institution reasonably expect to obtain a copy of the document upon request? (Citations omitted)

[55] I also refer to the judgment of the Court of Appeal in *Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner)* (*OCCRB*) holding that an institution may not avoid its obligations under *FIPPA* by failing to make appropriate contractual arrangements with an independent contractor covering information under its control. The *OCCRB* case involved a request for access to audio tapes of proceedings of the Ontario Criminal Code Review Board prepared by a private court reporting service. The Board argued that the tapes were not under its control because the court reporter was an independent contractor retained to prepare transcripts and there was no contractual provision giving the Board the right to possess the audio tapes. The Court rejected these arguments, holding that it was part of the Board's core mandate to keep a record of its proceedings which, at law, must remain under the Board's control. The Court stated:

> It is reasonable to expect that the Board would ensure, by contract if necessary, that any records of proceedings, backup records included, be used solely for the purposes of the Board. The Board can and should exercise control over the use of all records made by court reporters of its proceedings.
>
> . . . [T]he Board cannot avoid the access provisions of the *Act* by entering into arrangements under which third parties hold custody of the Board's records that would otherwise be subject to the provisions of the *Act*.
>
> Although the court reporter is an independent contractor, she plays an integral part in fulfilling the mandate of the Board under the *Criminal Code*. The court reporter has no independent role. She does not operate "independently or at arms length" from the Board.[5]

(ii) Analysis

[56] It is apparent that the personal information of CRR patrons and of OLG self-exclusion registrants was in the physical custody of CHC at the time of the hacking incident. The question remains whether OLG nonetheless had control of the personal

---

[5] *Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner)*, [1999] O.J. No. 4072 (C.A.) at paras. 32, 36-37.

information within the meaning of the *Act*.[6]

[57] OLG is exclusively authorized under the *OLGCA* to conduct and manage gaming at the Casino on behalf of the province. OLG's corporate objects specifically include providing for the operation of any business related to the operation of the gaming activities at the Casino that offers goods and services to its patrons. According to its annual reports, OLG "owns and manages" several casinos, including CRR, and has entered into agreements with private companies to carry out the day-to-day operations of these facilities.

[58] In addition, OLG is required to ensure that gaming activities at the Casino are conducted, managed and operated according to the *Gaming Control Act*, which authorizes the Registrar of Alcohol, Gaming and Racing to establish standards and requirements, such as the Gaming Standards. Standard 1.37 requires OLG and operators of gaming sites, such as CHC, to comply with the protections set out in *FIPPA* with respect to player personal information. This Standard also limits the purposes for which player personal information may be used to those necessary for "OLG's business" and require OLG's approval for any uses beyond these. In addition, OLG's MOU with the Ministry of Finance acknowledges that it is subject to *FIPPA* and that the property and/or services it orders or purchases are for the use of Ontario.

[59] With respect to OLG self-exclusion registrants, Standard 2.6 requires OLG to provide a voluntary self-exclusion program to allow individuals to exclude themselves from any or all gaming sectors, including casinos such as CRR. This Standard also requires operators of gaming sites, such as CHC, to operate this program on behalf of OLG by actively identifying registrants and, if required, denying them entry or removing them from premises.

[60] In my view, the above stipulations and requirements in the Gaming Standards and OLG's MOU with the Ministry of Finance support, if not entail, the conclusion that records generated in connection with various aspects of the Operator's core services under the Agreement must be considered to be under the control of OLG.

[61] The terms of the Agreement also support this conclusion. The Agreement provides that the Operator is the agent of OLG for the purpose of operating the gaming and related activities of the Casino and is an independent contractor for the purpose of operating the Complex on OLG's behalf. I note that, apart from this distinction, the Agreement does not elsewhere differentiate between the Operator's role as independent contractor or agent, including in relation to its management of customer

---

[6] An institution may also have legal custody over records containing personal information, even where it does not have physical custody. For the purposes of this report, it is sufficient to establish that the personal information is under the control of OLG within the meaning of the *Act*.

information on behalf of OLG.

[62] Under the Agreement, the Operator is obliged to operate the Casino Complex, which includes the Casino, in compliance with all applicable law and to provide for its proper, efficient and secure operation. The Operator is also obliged to comply with approved operating policies for both gaming and non-gaming activities and to make all records, reports and accounts relating to the operation of the Complex available to OLG for inspection. In addition, all intellectual property developed for use in the complex is the property of OLG. The same is true for the Customer Database which must be maintained confidential and secure, with exclusive rights to the Database to be transferred to OLG on termination of the Agreement. Similarly, all Complex Assets which, in my view, must include customer information, are the sole and exclusive property of OLG.

[63] On termination of the Agreement, the Operator must turn over possession and control of all Complex Assets to OLG, including all books, records and accounts. Further, the Operator must cooperate with OLG by providing information to prospective operators in the event of a competition to replace the Operator. The Agreement provides that the following categories of information and assets are the property of OLG: (i) all Intellectual Property which includes "all data bases" developed for use in conjunction with the Casino Complex; (ii) all Complex Assets which includes "all personal property and other assets" used in connection with the Complex; and (iii) the Customer Database for the Complex which the Operator is obliged to "continue to develop and maintain" presumably with new or updated patron information.

[64] There is nothing in the Agreement to suggest that these provisions are not broad enough to encompass the personal information at issue. It should be noted here that, apart from maintaining that the patron information which was unlawfully accessed was contained on a server separate from the Customer Database, OLG offers no evidence of, or justification for distinguishing the personal information of CRR patrons in the Customer Database from the personal information of CRR patrons in the compromised fileservers. Given the broad scope of OLG's property interests reflected in these provisions, there appears to be no valid basis for distinguishing between control over the unlawfully accessed patron information and the information in the Customer Database. Nothing in the Agreement suggests, for example, that the Operator is not obliged to turn over to OLG, or is entitled to retain, any information concerning CRR patrons on termination of the Agreement, whether or not it is part of the Customer Database. The Agreement specifically indicates that the opposite is the case.

[65] Significantly, OLG is the source of information concerning self-exclusion registrants, which goes beyond CRR patrons to encompass individuals who wanted to exclude themselves from being customers of any casino operated on OLG's behalf. Nothing in the Agreement suggests that OLG would not retain ownership or control of this information.

[66] OLG acknowledges that, like the Alcohol and Gaming Commission of Ontario

(AGCO), it had a right of access to some of the personal information that was unlawfully accessed, but states that this is commonplace with many regulated industries. OLG then compares this right of access to the right of access that the federal Financial Transactions and Reports Centre of Canada (FINTRAC) has over some of the same personal information. FINTRAC is the federal regulatory agency, established under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (*PCMLTFA*), to monitor public and private entities that handle large sums of money.

[67] A fundamental defect in this submission is that the Casino is not simply a member of a regulated industry subject to OLG oversight in the way, for example, that financial institutions, insurance companies and securities dealers are subject to FINTRAC's reporting requirements under the *PCMLTFA*. Rather, the Casino is the very business that OLG is solely empowered to "conduct and manage" under s. 207(1)(a) of the *Criminal Code*. Further, OLG's objects under the *OLGCA* include "provid[ing] for the operation of any business that the Corporation considers to be reasonably related to operating a gaming site or lottery scheme, including any business that offers goods and services to persons who play lottery schemes in a gaming site." OLG is thus clearly empowered to conduct and is ultimately responsible for both the gaming and customer related non-gaming business activities of the Casino.

[68] The importance of this distinction is explained in FINTRAC's website under the heading "Reporting Entities: Casinos."[7] The following description from the website makes it clear that it is the provincial lottery corporation responsible for casino gaming activities, and not the entity contracted to operate the casino on a day-to-day basis, that is the reporting entity responsible for ensuring compliance with the *PCMLTFA* and Regulations:

> The Regulations refer to the term **'conduct and manage'** to identify the entity legally responsible for the gaming activities **at a casino**. The definition is in line with the *Criminal Code* terminology that sets out who can oversee, carry out or license out the gaming activities (lottery schemes). The entities that conduct and manage lottery schemes, as authorized by the Criminal Code, must do so in line with the provincial legislation on gaming.
>
> In Canada, the provincial and territorial governments delegate the legal responsibility as to **who** can conduct and manage gaming activities (lottery scheme) at a casino. The entity that is delegated this responsibility by the province or territory is then responsible for meeting the obligations of the *PCMLTFA* and Regulations for that casino.

---

[7] See http://www.fintrac.gc.ca/re-ed/casinos-eng.asp.

> In some cases, the entity that **conducts and manages** a casino is not necessarily the same entity that operates the casino activities on a day-to-day basis. For example, if a provincial government has delegated the responsibility to conduct and manage the lottery scheme to a provincial lottery corporation who then delegated their reporting under the *PCMLTFA* to another entity, the provincial lottery corporation remains the reporting entity responsible for ensuring compliance with the *PCMLTFA* and Regulations. In other words, the legal entity responsible for the casino, as per the *PCMLTFA*, may choose to delegate the reporting to another entity but they remain responsible for meeting these obligations. (Original emphasis)

[69] Similarly, OLG has delegated to CHC its day-to-day functions of managing the gaming and related services offered to CRR patrons and OLG self-exclusion registrants, which includes handling their personal information. In the same way that OLG remains responsible for the reporting requirements under the *PCMLTFA*, OLG remains responsible for meeting its obligations under the *Act* in relation to the protection of that personal information.

[70] To borrow from the Court's reasoning in *OCCRB*, while the Operator may be an "agent" in some respects and "independent contractor" in others, it plays an integral part in fulfilling the mandate of OLG under the *OLGCA*. The Operator has no independent role and does not operate "independently or at arms length" from OLG. Based on the statutory and regulatory regime governing OLG's responsibility to conduct, manage and provide for the operation of the Casino, the personal information of CRR patrons and OLG self- exclusion registrants clearly relates to OLG's gaming responsibilities and related business activities. Further, considering the contractual and other material I have reviewed, OLG could reasonably expect to obtain copies of records containing this information from CHC on request.[8] For all of these reasons, and applying the test for control in the *Ministry of National Defence* case, I conclude that the personal information of CRR patrons that was accessed in the attack and the personal information of OLG self-exclusion registrants that was stored on compromised IT systems was under the control of OLG for the purposes of the *Act*.

Issue 3: Did CRR have reasonable measures in place to prevent unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with section 4(1) of Regulation 460 of the *Act*?

[71] Section 4(1) of Regulation 460 of the *Act* states:

---

[8] "Record" is defined at section 2(1) of *FIPPA* to include information recorded "by electronic means" and includes "a machine readable record." This would encompass any servers maintained by the Operator on which patron data is stored.

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[72] From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.

[73] Furthermore, simply because a breach occurred does not by itself mean that reasonable measures were not in place. The standard set out in section 4(1) is not perfection but reasonableness. It is therefore possible for records to be accessed in an unauthorized manner and yet the measures in place still be reasonable.

[74] The records at issue in this investigation are electronic records of CRR patrons and OLG self-exclusion registrants containing sensitive personal information of various types. One type is personal information that could be used to commit identity fraud against an individual. This is found in the records of personal information of CRR patrons. Information consisting of name, date of birth, address, social insurance number, driver's license number or other government-issued ID, signature, bank account numbers and credit application information could be used by an identity thief to steal an individual's identity and impersonate them to obtain false credit or other fraudulent benefits.

[75] The records also contain personal information of a type that could lead to the embarrassment or stigmatization of individuals. This is found in both the records of personal information of CRR patrons and OLG self-exclusion registrants. A CRR patron's outstanding credit collection information may contain details of their financial history that they would not want shared with others. Incident reports and complaints about CRR patrons may also contain sensitive information, including personal health information such as medical injuries or mental health 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.

[76] A large number of individuals were affected by this breach. The personal information of approximately 10,990 individuals was released online, but it is possible that the hacker stole additional records that he did not release. CHC was not able to determine from its investigation which records had been stolen from the CRR network as part of the attack. Of the 10,990 individuals that are known to be affected, approximately 4,602 were current or former employees of CRR and the vast majority of

the remaining 6,388 affected individuals were CRR patrons. CRR audit files containing the personal information of OLG self-exclusion registrants were housed on the same fileserver from which the hacker is known to have stolen CRR data.

[77] OLG and CHC submit that at the time of the cyberattack, CRR had reasonable safeguards in place to prevent unauthorized access to personal information and that its response to the incident was timely, comprehensive and effective in minimizing the risk of harm to potentially affected individuals. Furthermore, OLG and CHC submit that post-breach CRR has implemented security enhancements to minimize to the best extent possible the risk of a further cyberattack.

[78] In answer to questions regarding the security measures in place at the time of the attack, OLG and CHC submitted the following list of steps and IT practices:

- Developing a comprehensive Information Technology Security Procedures document
- Deploying advanced security software on key servers and IT workstations
- Developing an organization-wide data governance policy
- Computer Use Agreements that must be signed by all employees with access to the CRR network
- Use of antivirus software on all workstations
- Use of web-filtering software
- Deployment of firewalls to protect CRR networks
- Segregation of sensitive data, with access restricted to employees who required the data for legitimate business reasons and
- Limiting remote access to CRR systems to select individuals who require remote access for business reasons

[79] My analysis of the issue will focus on two aspects of the cyberattack: Casino Rama IT's response to the phishing email and its investigation of the remote connection. While in both cases I find shortcomings in the security measures in place, it is possible that each case taken on its own might not have constituted a contravention of section 4(1) of Regulation 460 of the *Act*. However, taking the cases together, I find that CRR did not have reasonable measures in place to prevent unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with section 4(1) of Regulation 460 of the *Act*.

Response to the Phishing Email

[80] The initial technique used by the hacker to gain access to the CRR network was the phishing email sent to 11 CRR employees on October 14, 2016. While the hacker used other techniques to move to other CRR systems and harvest credentials, his first foothold into the CRR network was by means of deception.

[81] The hacker appears to have used publicly available information from professional networking websites such as LinkedIn to research the organizational structure of CRR and use this knowledge to falsify a scenario in which a CRR manager sends an email to employees regarding a change in their work schedule. The hacker did a number of things to make the phishing email appear more realistic, including:

- creating a fake email account in the name of the CRR manager from a free email service;
- making the topic of the email a work-related issue; and
- disguising the malicious link as a CRR resource.

[82] As noted earlier, CRR had email security and firewalls in place as well as antivirus and antimalware software installed on employees' workstations, but none of these measures were able to detect the phishing email and prevent the hacker from gaining access to the CRR network. The employees who received the phishing email and clicked on the link embedded in it had malware executed and saved on their workstations.

[83] Once the malware was installed on CRR employees' workstations, the hacker then used it to gain further access to the CRR network. This raises an important concern about CRR's security posture at the time. The user accounts for CRR employees were granted what is known as "local administrator" privileges. What this means is that CRR employees had the technical ability to install software on their workstations, change their own configuration settings and access protected areas of the computer, even if this was not required for their job duties. Although CRR employees were required to sign a Computer Use Agreement prohibiting them from installing software on their workstations or altering any system configurations, technically they still had the ability to do so. The reason normal user accounts, including those of the employees who received the phishing email, were granted such privileges was that it was necessary to run several pieces of legacy software that were essential to CRR's operations at the time. If a user did not have local administrator privileges, the legacy software would not function properly on their workstation.

[84] I raise this point not to make a comment or finding about the particular software used by CRR. Each institution has its own business needs and each should be able to determine which tools are best suited to fulfill them. However, regardless of the choice of tools, each institution must conduct its operations in a secure manner and protect the confidentiality of the records under its control. By using legacy software that

required non- IT employees to have greater privileges than necessary for their job duties, CRR exposed its information holdings to an increased level of risk. The technical ability of CRR employees to change their own configuration settings and access protected areas of the computer could be exploited by hackers to assist them in moving to other systems on the network and harvesting credentials. In fact, this is what happened in the present case. The malware was able to run with elevated privileges upon execution, thereby providing the hacker with further means to attack the CRR network.

[85] By granting normal employees local administrator privileges for business reasons, CRR departed from a longstanding principle of computer security known as "least privilege." According to the U.S. National Institute of Standards and Technology (NIST), least privilege is the "principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function."[9] The importance of this principle is shown by its application in a number of security guidelines and standards. For example, the Australian Government's Cyber Security Centre has developed a list of eight essential strategies to mitigate cyber security incidents that it calls the "Essential Eight." One of these strategies applies the principle of least privilege, as follows:

> **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
>
> **Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.[10]

[86] In addition, the latest version of the AGCO's Gaming Standards from April 2017 contains additional requirements that were not set out in the Gaming Standards in effect at the time of the incident. The second requirement for Standard 1.20 in the updated Gaming Standards applies the principle of least privilege to restrict administrative privileges, as follows:[11]

> 1.20 **Access to gaming information systems shall be monitored, logged and shall be traceable to a specific individual.**
>
> **Requirements** – At a minimum:
>
> . . .

---

[9] See https://csrc.nist.gov/glossary/term/least-privilege.
[10] See https://acsc.gov.au/publications/protect/essential-eight-explained.htm.
[11] See https://www.agco.ca/sites/default/files/gaming_standards_apr-2017_en.pdf.

> 2. All system accounts (or other accounts with equivalent privileges) shall be restricted to staff that provide IT support, and mechanisms shall be in place to secure and monitor use of those accounts.

[87] Although CRR did not follow the principle of least privilege in certain respects, this by itself does not necessarily mean that CRR failed in its overall responsibilities to protect the records of personal information of CRR patrons and OLG self-exclusion registrants. Whether the security measures in place at the time reasonably protected the records at issue depends on whether they were sufficient given the increased level of risk from local administrator privileges being granted to CRR employees.

[88] In addition to email security and antivirus and antimalware software, CRR also had measures in place to educate and inform employees about threats posed by phishing emails. In their submissions, OLG and CHC provided examples of communications sent by Casino Rama IT to CRR employees about phishing awareness generally and specific email threats. The communications contain a number of recommendations and messages, including:

- Do not open any attachments and do not click any links in emails unless you are completely certain who the sender is;
- Some phishing emails may target specific employees and appear to come from managers or personal contacts;
- To help identify whether an email is legitimate, check the full email address of the sender and hover over links to display the actual web address in the status bar;
- If in doubt, call the sender for additional clarification or simply delete the email; and
- The IT help desk will never request employees to submit, validate or verify their account passwords.

[89] Although I agree with the advice in these messages, I note that none of the communications offer guidance as to what CRR employees should do in the event that they are tricked by a phishing email. While deleting illegitimate emails or contacting the sender when in doubt are preferred outcomes, there may be cases where individuals initially open attachments or click on links, but only realize afterwards that the resources were fraudulent and used as part of an attack.

[90] Again, this is what happened in the present case. At least one of the recipients of the phishing email contacted the CRR manager to report that the link to the updated holiday schedule did not work, meaning that they had clicked on the link and unbeknownst to them had malware installed on their workstation. In response, the CRR manager sent an email to all other CRR managers directing them to avoid clicking on

the link. However, simply notifying such individuals that the email was fraudulent and advising them to delete it or not to click on the link does not address the fact that they may have already fallen prey to the attack.

[91] This strikes me as a significant gap in the communications sent to CRR employees, especially given the heightened level of risk in CRR's security posture. If an individual realizes that they have been deceived by a phishing email, they should immediately report this to their IT department. Doing nothing or deleting the email after the fact only helps to conceal the breach to the advantage of the hackers. Indeed, if the individuals who clicked on the malicious link had reported it to Casino Rama IT, Casino Rama IT would have been in a better position to understand full size and scope of the cyberattack, including the implications of the remote connection (discussed below).

[92] Given this gap, it is perhaps not surprising then that none of the CRR employees who received the phishing email or clicked on the link contacted the IT Help Desk to report it. However, Casino Rama IT still became aware of the email, as their managers received the following warning email sent by the CRR manager:

> To all,
>
> Please be advised that you may be receiving an email from what appears to be my account under the heading Holiday Schedule. This is spam. If you receive it please do not go to the link.
>
> Thank you.

[93] According to CRR's IT Security Procedures under the section "Problem and Incident Management,"

> If Users bypass the Help Desk and contact the ASG [Application Support Group] and Tech groups directly, staff will assist them as required but also advise that future requests for support should be directed to the IT Help
>
> Desk. ASG and Tech groups will be responsible for notifying IT Ops for any High Severity incidents where they were the initial point of contact. (p. 22)

[94] Despite this procedure, Casino Rama IT decided not to commence an investigation into the phishing email. In their representations, OLG and CHC stated:

> No additional investigation was commenced by IT, as a warning not to open the email had already been sent, and they believed the information security measures they already had in place were sufficient to prevent harm if an employee did open it.

[95] This is a problematic decision. From the description provided in the CRR

manager's warning, it is clear that the email was not a generic phishing email written from the perspective of a third party and applicable to any number of individuals or organizations. It was designed to impersonate a specific CRR manager and to be sent to CRR employees with the goal of deceiving them with a work-related matter. Phishing emails of this type that target specific individuals and/or organizations are known as "spear" phishing emails.

[96] The threat posed by spear phishing emails is generally greater than that of generic, non-targeted emails. Spear phishing emails are not only customized to a particular individual and/or organization, which helps increase their believability; the customization involved in their design indicates a motivated attacker with the potential to carry out a sophisticated attack. Especially in cases where they have been successful in tricking their targets, the severity of the threat posed by spear phishing emails is potentially high.

[97] According to OLG and CHC, one of the reasons Casino Rama IT decided not to investigate and evaluate the threat of the spear phishing email was that they believed the security measures in place were sufficient to protect against it. However, in one of the phishing awareness communications sent to CRR employees, Casino Rama IT describe the level of protection offered by their email security as follows:

> We have software in place that filters all email, however the challenge is to identity and segregate the fraudulent email from legitimate email. This is not an easy process as unfortunately the people that generate the fraudulent mail are familiar with the algorithms used by the email filtering software and are constantly finding ways around it.
>
> In recent emails, you will often see an attachment with the filename such as *filename.zip.txt*. The *.zip.txt* extension actually indicates that our system has identified potential malware and already removed the original attachment. It does allow the mail to go through to allow the user to see it just in case it was legitimate, in which case the user can contact the sender and have them re-send the attachment in another format.
>
> Unfortunately, this will be a cat and mouse game for ever and ever. Here is a general rule of thumb: If you do not know who the email sender is, DO NOT OPEN ANY ATTACHMENTS AND SIMPLY DELETE THE MAIL. The hackers are counting on you succumbing to curiosity – simply ignore the temptation.

[98] This illustrates an important point about the limits of algorithmic security tools, which include the antivirus and antimalware software installed on CRR employees' workstations. Such tools are effective to the extent that the future looks like the past. So long as the inputs they receive follow the same patterns of examples they have seen in the past, they work as expected. However, if new patterns or examples are introduced, they may not be as effective. Thus, if a hacker wanted to evade one of

these systems, what he may try to do is present it with an example that it has not yet seen or mimic the inputs of a "safe" resource, in the hopes that the system will misclassify it. As the system updates its algorithm, hackers will attempt to discover new ways around it, and the cycle continues in a "cat and mouse game." In saying this, I do not mean to suggest that such tools have no utility or that they are not part of a program of reasonable security measures. Rather, the point I want to make is that they are no "silver bullet" and an organization must be aware of the limits of these tools and ensure that they are used in conjunction with other security measures. CRR makes the same point in its own communication above.

[99] It is useful at this point to recap some of the findings that have been made with respect to CRR's response to the phishing email:

- The records at issue were electronic records containing sensitive personal information of a large number of CRR patrons and OLG self-exclusion registrants;
- Non-IT CRR employees were granted local administrator privileges on their workstations, increasing the level of risk in CRR's security posture;
- None of the phishing awareness communications sent to CRR employees offered guidance as to what to do in the event that they are tricked by a phishing email;
- The phishing email was a spear phishing email designed to target CRR and specific CRR employees;
- Algorithmic security tools, including the email security and antivirus and antimalware software installed on CRR employees' workstations, are limited in terms of their ability to detect malicious emails and software; and
- Casino Rama IT did not investigate the spear phishing email after becoming aware of it.

[100] Based on the above, I have concerns about the reasonableness of the security measures in place at CRR to prevent unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants. Although a limitation in one area of a security program may not be fatal if accompanied by other measures to support the overall security of the system, the circumstances surrounding Casino Rama IT's response to the phishing email suggest that additional measures may have been needed to provide reasonable protections, taking into account the nature of the records, including their sensitivity, level of risk and the types of threats posed to them. At the same time, I recognize the sophistication of the attack, including the tools and techniques used by the hacker to gain access to the CRR network. Faced with a motivated intruder with the skills and capacity to carry out a multistage attack, the shortfalls in Casino Rama IT's response to the phishing email and security measures may not on their own have constituted a contravention of section 4(1) of Regulation 460 of the *Act*. However, as discussed below, added to these shortfalls were problems

in the investigation of the remote connection.

Investigation of the Remote Connection

[101] Casino Rama IT first became aware of suspicious activity on the CRR network through a chance occurrence. On October 19, 2016, an employee reported that she was prevented from logging in to her workstation because the user account of a Casino Rama IT staff member was already logged in to it remotely. However, Casino Rama IT determined that the particular IT staff member was not responsible for the remote connection and began an investigation into the incident.

[102] Following CRR's IT Security Procedures, the incident was logged in an incident-tracking database. Throughout the investigation, the incident was classified as having "Low" severity and as being "No" security incident. A timeline of the investigation is as follows:

- On October 19, 2016, Casino Rama IT installed new antivirus software on the employee's workstation, began analyzing security log files, found that Dropbox had been installed on the employee's workstation and determined that no data had been uploaded to Dropbox as access to the service from the employee's workstation was already blocked by CRR's firewall;

- On October 19 and 20, 2016, Casino Rama IT blocked access to Dropbox from all computers on the CRR network and disabled the remote desktop program;

- On October 21, 2016, administrator, exchangeserver, firewall and router passwords were changed; and

- On October 27, 2016, Casino Rama IT conducted a port scan of the employee's workstation, identified a Russian IP address attempting to communicate with the employee's workstation and blocked communication with that IP address using CRR's firewall.

[103] The key step that enabled Casino Rama IT to discover the Russian IP address and to contain the cyberattack by blocking it was their decision to conduct a port scan of the employee's workstation. However, the period from first detection of suspicious activity to deployment of the port scan was eight days. If the threat posed by the remote connection had been taken more seriously and a full diagnostic assessment had been conducted at the beginning of the investigation, it likely would have led to an earlier containment of the cyberattack, potentially mitigating its effects, even though Casino Rama IT did not become aware of the fact that CRR data had been stolen by other means and that 38 other systems had been compromised until after the hacker's emails.

[104] In answer to questions regarding the timing of the port scan, OLG and CHC submitted:

> Although Casino Rama IT believed that the steps taken on October 19 and 20 had resolved the issue on Employee C's workstation, as a precaution a week later, on October 27, they performed a remote port scan. This port scan identified a Russian IP address [] attempting to communicate with Employee C's workstation; communication with that IP address was immediately blocked using Casino Rama's firewall.

[105] In answer to a series of follow-up questions regarding the circumstances of the port scan, OLG and CHC submitted:

> Casino Rama IT staff began their investigation of the remote connection to Employee C's computer immediately after it was reported. Among other things, this investigation involved reviewing log files and analytics generated by [security management software]. The process of reviewing these materials, particularly the voluminous log files, took considerable time.
>
> When Casino Rama IT staff were not able to determine the source of the remote connection to Employee C's computer from their review of the [] analytics and log files, they decided to perform a remote port scan. Performing a remote port scan is considered a secondary step in investigating an incident of this nature, so the primary investigative tools were exhausted before moving on to this intermediate step.

[106] I do not accept that the above steps amount to a timely and appropriate response to an incident of this nature. What the suspicious remote connection to the employee's workstation revealed was that the credentials of a Casino Rama IT staff member had been compromised and that an unknown individual had had full control over an employee's workstation. This is an alarming situation. In these circumstances, I disagree with Casino Rama IT's assessment of the adequacy of the initial steps it took in response to the remote connection. According to OLG, Casino Rama IT believed that it had "resolved the issue" after it had:

- blocked access to Dropbox from all computers on the CRR network;
- disabled the remote desktop program; and
- changed administrator, exchangeserver, firewall and router passwords.

[107] While these measures would have prevented a second remote connection of the same kind, what they did not address is how the suspicious remote connection came to happen in the first place. In particular, they did not address how the credentials of the Casino Rama IT staff member whose user account was used to log in to the employee's workstation were compromised. Without an understanding of this aspect of the remote connection, 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.

[108] Indeed, further evidence of the low priority with which the incident was handled is shown by the initial advice Casino Rama IT provided to the employee upon learning of the remote connection. After hearing that a Casino Rama IT staff member was preventing the employee from accessing her computer, Casino Rama IT initially logged the incident as follows:

> 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.

[109] 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 antivirus 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-the-fact "precaution."

[110] It is useful to note that the Gaming Standards take a similar, contextual approach to setting requirements for investigations of suspicious incidents. Standard 1.27 provides as follows:

> 1.27 **Security activities shall be logged in an auditable manner, monitored, promptly analyzed and a report prepared and escalated as appropriate.**
>
> **Requirements** – At a minimum:
>
> 1. Attempts to attack, breach or access gaming system components in an unauthorized manner shall be responded to in a timely and appropriate manner.
>
> 2. Intrusion attempts shall be actively detected and where possible prevented from causing disruption or outage of the gaming system.
>
> 3. There shall be adequate logging to capture and monitor any attempts to attack, breach or access in an unauthorized manner any components of the gaming system. There shall be an appropriate escalation procedure.

[111] The Standard does not list specific steps that must be taken or tools that must be used, leaving phrases such as "timely and appropriate manner," "actively detected" and "appropriate escalation procedure" undefined. Rather, it looks to the circumstances

at hand and the nature of the security incident to determine what constitutes a reasonable response to it.

[112] Based on the above, I have concerns about the reasonableness of Casino Rama IT's investigation of the remote connection. To wait eight 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 be a timely or appropriate response to an incident of this nature. At the same time, it must be acknowledged that Casino Rama IT did in the end employ diagnostic tools that led to the discovery of the Russian IP address. It is a fine line to draw when the difference between reasonable and unreasonable is only a matter of days, although every minute counts within the context of a breach.

Taking the cases together

[113] While both Casino Rama IT's response to the phishing email and its investigation of the remote connection reveal shortcomings in its security measures, it is possible that each flaw taken on its own might not have constituted a contravention of section 4(1) of Regulation 460 of the *Act*. However, the cumulative effect of these deficiencies amounts to a failure to have in place reasonable measures to prevent and mitigate unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants, as required by section 4(1) of Regulation 460 of the *Act*.

[114] However, since the breach, CRR has taken steps to address the gaps in its systems and processes that were exploited by the hacker's phishing email. Some of the measures include working to remove local administrative privileges from normal user accounts, changing CRR's procedures to ensure Casino Rama IT investigates all suspicious emails of which it becomes aware and blocking executable files on the firewall. I am satisfied with CRR's response to the breach in this regard, although I would recommend in addition that Casino Rama IT include in its phishing awareness communications guidance to the effect that if a CRR employee realizes that they have been deceived by a phishing email, they should immediately report this to Casino Rama IT.

[115] With respect to its investigation of the remote connection, CRR has updated the security measures in place to include additional controls, such as developing a specific IT incident response plan, defining separate privileged accounts for administrative activities, implementing two-factor authentication for system administrators and limiting administrator account access to specific jump servers within the CRR network. I am satisfied with CRR's response to the breach in this regard.

Issue 4: Did OLG have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with the requirements of the *Act* and its regulations?

[116] Where an institution subject to the *Act* retains a private sector entity to perform core functions on its behalf, it must take all reasonable and appropriate measures to ensure that the entity deals with the records under the control of the institution in ways that comply with the institution's obligations under the *Act*. The principal means by which the institution may achieve this objective is through provisions of its contract with the private sector entity that ensure that the services performed on the institution's behalf comply with the rules and safeguards set out in the *Act*. Audits are another necessary and important way to ensure adequate oversight and compliance with the institution's obligations. Implementation of audits should also be expressly provided for and made enforceable under the terms of the agreement between the institution and the private sector entity.

[117] The above-noted principles and examples of the types of contractual provisions which should be in place for records of personal information are described in Privacy Investigation Report PC12-39, *Reviewing the Licensing Automation System of the Ministry of Natural Resources, A Special Investigation Report* (MNR Report).[12] One of the issues considered in that report was whether an agreement with a private sector company for the operation of the Ministry of Natural Resource's hunting and fishing Licensing Automation System (LAS) was adequate for the purposes of the *Act*. The relevant passages are set out here.

> **The Contract**
>
> . . . Organizations must take reasonable steps to reduce the likelihood of a breach, wherever the information may be held. This becomes especially important when government information management functions are outsourced to private sector agents. In these cases, the reasonable measures required under the *Act* and its regulations include appropriate contractual provisions that ensure accountability, privacy and security. Therefore, whether the Ministry has discharged its obligations to ensure that all reasonable steps have been taken to protect the personal information under its control must be assessed in view of its agreement with the Agent.

[12] Privacy Investigation Report PC12-39, *Reviewing the Licensing Automation System of the Ministry of Natural Resources, A Special Investigation Report*, June 27, 2012, at pp. 7-8.

I have carefully reviewed the Ministry's agreement with the Agent, including the contract and all appendices and schedules. The Ministry's contract includes robust provisions that protect the personal information under its control and restrict the use of that information by the Agent. In this regard, the following provisions of the contract are relevant:

a) *Ownership* – The contract states that the Ministry shall be the owner of all Ministry data. Ministry data is defined in the contract to include: all data created or modified by the LAS as well as the data relating to licence issuers and angler and hunter licence records, including all data created, modified, collected and stored in the LAS database and any legacy data.

b) *Collection, Use and Disclosure* – The contract states that the Agent cannot directly or indirectly use, collect or disclose any personal information for any purposes not authorized by the Ministry. In particular, the Agent has acknowledged in the contract that unless it obtains specific, written pre-authorization from the Ministry, any access to or use of the Ministry's property, technology or information that is not necessary for the performance of its contractual obligations with the Ministry is strictly prohibited. These restrictions would prohibit the Agent's sale of personal information without the Ministry's consent.

c) *Confidential Information* – Confidential information is defined in the contract to include all personal information that the Ministry is obliged, or has the discretion not to disclose under provincial or federal legislation or otherwise at law. The Agent's contractual obligations for this information include:

i) keeping the information confidential and secure;

ii) limiting the disclosure of confidential information to only those who have a need to know it for the purpose of the contract and who have been specifically authorized to receive such disclosure; and

iii) not directly or indirectly disclosing, destroying, exploiting or using any confidential information (except for the purpose of the contract, or except if required by order of a court or tribunal), without first obtaining the written consent of the Ministry and in respect of any of the Ministry's confidential information about any third party, the written consent of such third party.

It is important to note that these restrictions would also prohibit the Agent's sale of personal information without the consent of the Ministry and relevant third party.

d) *Notice of Compelled Disclosure* – If the Agent is legally compelled to disclose any of the Ministry's confidential information, the Agent must provide the Ministry with prompt notice to allow the Ministry to seek a protective order or other appropriate remedy to prevent or limit such disclosure. Further, the Agent will disclose only that portion of the confidential information which the Agent is legally compelled to disclose.

e) *Subcontracting* – The contract states that the Agent is not permitted to subcontract the whole or any part of the contract without the prior written consent of the Ministry. If the Ministry does consent to the Agent subcontracting certain services, the Ministry may impose the same contractual obligations on the subcontractor that were imposed on the Agent.

f) *Security* – The contract states that the Agent must ensure the security and integrity of all personal information and records in its possession. The Agent must keep the personal information and records in a physically secure and separate location, safe from loss, alteration, destruction or intermingling with other records and databases. Further, it must implement, use and maintain the most appropriate products, tools, measures and procedures to do so. The Agent has also provided the Ministry with point-of-sale devices that incorporate reliable security, including secure operating and control systems that prohibit any incoming connection to the devices.

g) *Retention and Destruction* – The contract states that the Agent must return all of the Ministry's confidential information to the Ministry before the end of the term of the contract, with no copy or portion kept by the Agent. The Ministry has also stated that it has initiated the development of a retention and destruction schedule with the Agent. The Ministry expects the retention and destruction schedule to be completed by the spring of 2013.

h) *Audits* – The contract states that the Agent will comply with annual audits for privacy and security compliance, for the duration of the contract. These audits may include reviews of threat risk assessments, Privacy Impact Assessments (PIAs) and vulnerability assessments.

> i) *Governing law* – The contract clearly states that the governing law of the contract is Ontario and the federal laws of Canada.
>
> With the exception of retention and destruction of the Ministry's data, the Ministry's contract with the Agent demonstrates that the necessary provisions are in place to strongly safeguard the privacy and security of personal information collected under the hunting and fishing licensing program. . . . (Emphasis in original removed)

[118] Based on the framework set out in the MNR Report, our request for information letter of June 14, 2017 asked OLG to address the following series of questions:

> 5. Please specify the provisions of any agreement(s) between OLG and the Operator governing the personal information of Casino patrons, players and staff. In particular, specify any provisions governing the following issues:
>
> ● Confirming OLG ownership/control of personal information collected, created, modified and/or stored by the operator.
>
> ● Requiring compliance by the operator with Part III of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and associated regulations in relation any personal information holdings.
>
> ● Limiting the collection, use and disclosure of personal information for authorized purposes and by authorized staff.
>
> ● Maintaining the confidentiality and security of the information (e.g. secure storage and transmission, encryption, authentication for access.)
>
> ● Allowing any subcontracting of services involving the handling of personal information.
>
> ● Setting out the means for dealing with the compelled disclosure of personal information to third parties (e.g., courts, law enforcement).
>
> ● Setting out retention schedules, requiring secure destruction.
>
> ● Mandating periodic OLG audits of operator for privacy and security compliance, including review of any threat risk assessments, privacy impact assessments.

> ● Requiring the training of operator's staff and management in *FIPPA* requirements and security measures; designation of operator privacy officer.
>
> ● Providing for the disposition of personal information on termination of the agreement (return or secure destruction).
>
> ● Referring to any other applicable laws.

6. What measures were/are in place for implementing, administering and enforcing contractual provisions relating to the protection of personal information?

7. Apart from any contractual provisions, what (if any) other policies, protocols or practices were in place at the relevant times regarding OLG's oversight, administrative controls, monitoring, auditing and/or reporting requirements, with a view to ensuring compliance with the privacy provisions of *FIPPA*?

8. Please provide unsevered copies of all agreements, policies and other supporting documents (including the Interim Operating Agreement for Casino Rama Execution Version dated August 1, 2011).

[119] OLG's answers to these questions are set out here in part:

Questions 5 and 8:

. . . Section 6.4 of the Interim Operating Agreement addresses the ownership, development, maintenance, and use of Casino Rama's customer database. In addition, in accordance with section 2.13(c) of the Interim Operating Agreement, CHC is required to comply with all Applicable Law, including:

> a) the federal *Personal Information Production and Electronic Documents Act*, which applies to CHC as a private sector enterprise; and
>
> b) IT security controls and requirements for player personal information imposed under the *Gaming Control Act*, and enforced by the Alcohol and Gaming Commission of Ontario (AGCO) discussed further below.

. . .

Questions 6 and 7:

OLG exercises oversight over the operations of Ontario's resort casinos, including Casino Rama, in order to ensure the operators' compliance with their contractual and regulatory obligations and, in turn, OLG's compliance with the privacy provisions of *FIPPA*. Casino Rama is also subject to regulation by the AGCO, including regulation of IT security standards.

OLG exercises oversight over Casino Rama's operations through, among other measures:

1) reliance on internal and external audits;

2) relationship management;

3) annual budget approval; and,

4) reliance on CHC's compliance framework.

Further details of OLG's oversight role and the AGCO's regulatory work are set out below. As noted above, the next generation of operating agreements for Ontario resort casinos will include additional specific provisions relating to IT security and privacy.

AGCO regulation of IT security. A resort casino operator is a registrant under the *Gaming Control Act* subject to the jurisdiction and oversight of the AGCO. In carrying out its oversight role, OLG relies on the work of the AGCO and seeks — whenever possible — to avoid unnecessary duplication of AGCO efforts directed at ensuring compliance.

As a registrant, each resort operator is required to comply with the requirements of the *Gaming Control Act,* including requirements relating to IT security and protection of customer data. Registrants also must cooperate with the AGCO in its investigations, audits, and reviews to ensure compliance with the [*Gaming Control*] *Act.* Failure to comply with the [*Gaming Control*] *Act* can result in the AGCO denying registration or renewal of registration.

Prior to the transition to the risk-based *Registrar's Standards for Gaming* (the "Gaming Standards") in 2016, all operators were required to submit control activities to the AGCO for approval prior to transitioning to a standards-based framework. The AGCO approved each operator's Internal Control Manual (ICM) and changes thereto. Operators were, in turn, expected to conduct gaming operations against the approved ICM. The ICM, as updated from time to time, sets out the procedures to be followed in respect of a wide range of practices. All operators were subject to

> regular inspections and investigations by the AGCO, including periodic audits.
>
> . . .
>
> ***Reliance on external and internal audits.*** Pursuant to the Gaming Standards, CHC has implemented a three-year plan under which either its external or internal auditors tests each of its control activities. The audits cover all aspects of the casino's operations, including physical access and financial controls; compliance oversight; employee training; anti-money laundering reporting, vendor management and IT systems (including information security).
>
> OLG Audit Services holds quarterly meetings with each resort operator's internal audit team to ensure that resort operators have appropriate audit plans in scope each year. On an annual basis, OLG Audit Services reviews each operator's internal audit plans and provides advice regarding additional areas for audits to be considered.
>
> . . .

[120] OLG then goes on to outline for each of the remaining measures referred to above (under items 2–4) general aspects of OLG oversight of CRR's operations which do not specifically address the privacy or security of the personal information of CRR patrons and OLG self-exclusion registrants.

[121] My analysis of the issue will be divided into two parts, according to the types of protective measures available to institutions when outsourcing services involving the collection, use or disclosure of personal information. For the reasons set out below, I find that OLG did not have reasonable contractual nor reasonable oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants.

Contractual measures

[122] OLG's Agreement with CHC deals with the contractual elements set out in the MNR Report, albeit for the most part in an indirect manner only. There are no provisions in the Agreement specifically establishing or requiring measures to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants. The Agreement does not even mention the term "personal information," including in relation to the Customer Database. It is only incidentally or by way of reference to other laws that the Agreement speaks to the issues of privacy, security and accountability.

[123] For example, the Agreement provides that the Operator is required to comply with all Applicable Law and defines this term in a manner that includes "any . . . binding

directives issued by the Gaming Commission." The AGCO's Gaming Standards set out standards and requirements relating to IT security management and data governance that deal with a number of issues described in the framework of contractual provisions set out in the MNR Report. Some of the relevant standards and requirements from the AGCO's Gaming Standards include, in part:

> 1.14 **Compliance with the Standards and Requirements shall be documented in an organized manner to ensure that the information is capable of being reviewed and audited by an independent oversight function.**
>
> **Requirements** – At a minimum:
>
> 1. Documentation shall be reviewed and analyzed to ensure compliance with the Standards and Requirements, and approved by management.
>
> 2. Internal and external auditors shall be granted access to all relevant systems, documentation (including control activities) and resources for the purpose of conducting an audit. . . .
>
> 1.19 **Users shall be granted access to the gaming system based on business need.**
>
> **Requirements** – At a minimum:
>
> 1. Access privileges are granted, modified and revoked based on employment status and job requirements and all activities associated with these actions are logged.
>
> 2. Access privileges are independently reviewed and confirmed on a periodic basis.
>
> 1.26 **Gaming systems, infrastructure, data, activity logs and all other related components shall be protected from threats, vulnerabilities, attacks or breaches.**
>
> **Requirements** – At a minimum:
>
> 1. All users shall be authenticated.
>
> 2. All components shall be hardened in accordance with industry and technology good practices prior to going live and prior to any changes.
>
> 3. The appropriateness and effectiveness of steps taken to harden technology components shall be regularly assessed.

4. Patches to correct any security risks shall be updated regularly.

1.28 **Independent assessments shall be regularly performed by a qualified individual to verify the adequacy of gaming system security and all of its related components.**

1.36 **Sensitive data, including player information and data relevant to determining game outcomes, shall be secured and protected from unauthorized access or use at all times.**

. . .

1.37 **Player information shall be securely protected and its usage controlled by OLG.**

Requirements – At a minimum:

1. Data collection and protection requirements for player personal information shall meet those set out in the Freedom of Information and Protection of Privacy Act.

2. Player information shall only be used for OLG's business unless there is prior approval from OLG.

[124] These standards and requirements are appropriate and appear to function in place of specific contractual provisions to address the issues of collection, use and disclosure, confidential information, security and audits, as outlined in the MNR Report. CHC is required to comply with them as a condition of the Agreement. Moreover, they describe protections for the issues they address in a manner consistent with the requirements of the *Act*. Indeed, in one case, they even make explicit reference to it.

[125] However, as an external document, it is possible for the AGCO's Gaming Standards to change independently of the Agreement in a manner that makes the applicable standards and requirements no longer consistent with the *Act*. The Agreement simply references the AGCO's Gaming Standards in general terms. It does not refer to individual standards or requirements, nor does it include any in the body of the Agreement. In my view, minimum requirements would need to be explicitly incorporated into the Agreement in order for them to function as appropriate contractual provisions to ensure privacy, security and accountability. It is not enough to reference in general terms an external document in the Agreement for the purposes of the *Act*.

[126] As discussed below, it is apparent that OLG relies heavily on the regulatory functions of AGCO with respect to oversight measures governing the security of CRR patrons' and OLG self-exclusion registrants' personal information. While this may be a necessary facet of a regulatory regime governing the registration of operators of

gaming sites, it effectively cedes a large measure of the oversight function to an authority that does not have direct control over the personal information of CRR patrons and OLG self- exclusion registrants and the responsibility under the *Act* of ensuring the privacy and security of that information. AGCO's regulatory authority under the *Gaming Control Act* is ultimately limited to denying registration or renewal of registration. What is needed, in my view, are specific contractual terms providing for timely and effective remedies that can be invoked by OLG where the Operator fails to provide proof of substantial compliance with AGCO Audit Report recommendations: for example, in respect of establishing a proper a data governance framework. Provisions such as these are missing from the Agreement.

[127] Other issues outlined in the MNR Report appear in other parts of the Agreement. For example, the Agreement provides that the Customer Database, the Complex Assets and the intellectual property developed by the Operator in connection with the Casino Complex are the property of OLG and, further, provides for the confidential treatment of the Customer Database and restrictions on its use only in connection with the Operation of the Complex. The Agreement also provides that rights to this property are to be vested in OLG on termination and that the Operator will not remove or retain any copies of the Customer Database.

[128] Although these provisions appear to be designed primarily to protect OLG's commercial interests in CRR patron data, the Complex Assets and any intellectual property, they also incidentally deal with issues of ownership, retention and destruction. In my view, these provisions do not provide adequate protections to ensure privacy as they do not clearly apply to the full scope of data holdings in which the personal information of CRR patrons is stored. In answer to questions regarding the application of the *Act*, OLG and CHC submitted:

> [T]he Customer Database is not the sole repository of personal information of Casino Rama patrons. In the ordinary and necessary course of business, Casino Rama creates and stores other documents containing patron 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 servers that were accessed in the cyberattack. . . .
>
> The personal information accessed in the cyberattack was stored on two Windows servers . . . that house network folders in which Casino Rama employee documents are stored. The Customer Database is stored on an entirely different, non-Windows server. . . .
>
> We do not agree that the personal information of patrons that was accessed in the attack, or the IT systems or accounts that were

> compromised, were under the control of OLG at the time of the cyberattack . . . .

[129] Although, as I stated above, the terms of the Agreement dealing more generally with ownership of Complex Assets are, in my view, broad enough to cover all CRR patron data, 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 that demonstrates the lack of clarity in the Agreement.

[130] While the Agreement speaks to the issues of ownership, retention and destruction of the Customer Database, it remains silent on the other repositories of personal information of CRR patrons and OLG self-exclusion registrants. Without specific provisions dealing with all data holdings, the Agreement cannot be said to have appropriate contractual provisions in place to address the issues of ownership, retention and destruction. Greater clarity is needed in the Agreement to ensure the same rules explicitly apply to all patron information in OLG's control.

[131] The remaining issue outlined in the MNR Report is that of subcontracting. The Agreement provides that the Operator is not permitted to enter into any contract for goods, services or materials that is longer than 12 months or that costs more than $100,000 without the prior written approval of OLG. In my view, this provision falls short of providing an adequate level of protection for the personal information of CRR patrons and OLG self-exclusion registrants. For contracts under 12 months or for less than $100,000, it permits the Operator to subcontract duties described in the Agreement without any oversight or requirements to impose the same contractual obligations on the subcontractor. This allows for a scenario in which the personal information of CRR patrons and OLG self-exclusion registrants may potentially be used by a third party for unrelated purposes.

[132] Based on the above, I find that OLG did not have reasonable contractual measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with the requirements of the *Act* and its regulations. Although the Agreement deals with the contractual issues outlined in the MNR Report, the manner in which it does so is insufficient for the purposes of the *Act*.

[133] However, since the breach, OLG has committed to replacing the Agreement with new operating agreements that will have additional specific provisions relating to IT security and privacy. In the case of any future operating agreements, my recommendation would be the same: OLG should ensure that the agreements explicitly incorporate robust provisions to ensure that the services performed on its behalf comply the rules and safeguards set out in the *Act*, including provisions to address the issues of collection, use and disclosure, confidential information, security, audits, ownership, retention, destruction and subcontracting, as outlined in the MNR Report.

Oversight measures

[134] As noted above, OLG submits that, with respect to oversight measures, it relies on the work of the AGCO and seeks, whenever possible, to avoid unnecessary duplication of AGCO efforts directed at ensuring compliance and that all operators, including CHC, were subject to regular inspections and investigations by the AGCO, including periodic audits. OLG also submits that it relies on external and internal audits and that, pursuant to the Gaming Standards, CHC has implemented a three-year plan under which either its external or internal auditors tests each of its control activities.

[135] In response to a series of follow-up questions requesting any documents that provide examples of OLG's reliance on the AGCO's regulation of IT security as well as external and internal audits prior to the date of the breach, OLG provided copies of three documents:

- An AGCO audit report of CRR from 2015 (AGCO Audit Report);
- CRR's response to the AGCO Audit Report (CRR Audit Response); and
- A vulnerability assessment of CRR performed by OLG in 2011 (Vulnerability Assessment).

[136] The date of completion of the Vulnerability Assessment was more than five years prior to the date of the breach. In my view, this renders the assessment too old and outdated for it to be considered an example of an adequate oversight measure within the context of this investigation. In addition, the assessment was only partial in that it did not evaluate all aspects of the security controls and one system in particular was excluded from it.

[137] The AGCO Audit Report, which is dated May 19, 2015, covers various aspects of CRR's operations, including information security. The relevant findings and recommendations of the report are set out here, in part:

> **19. An IT management framework was not established.**
>
> **Risk Rating: Medium**
>
> . . .
>
> During the audit it was noted that an IT management framework had not been established and the management of IT processes was insufficient. Policies such as those for system patching and vendor management were not formally and adequately defined and documented.
>
> **<u>Root Cause and Impact</u>**

Casino Rama had not adopted an industry standard / framework for IT management. Existing IT resources were being utilized primarily to provide operational support.

Without a proper framework, the critical IT processes and controls required to meet business objectives, 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.

Recommendation

Casino Rama should adopt an industry standard / framework to implement adequate IT processes and controls and manage its IT control environment.

20. A Data Governance framework was not in place.

Risk Rating: Medium

. . .

To ensure that gaming related data is secure and appropriately managed at Casino Rama, a Data Governance ("DG") framework that includes documented policies, training and periodic review of data protection controls should be established. Specifically, all data should be classified based on its sensitivity and criticality. Data should have assigned owners accountable for the protection of the data.

During the audit it was noted that while Casino Rama had briefly defined data sensitivity and ownership, the overall DG framework had not been established. Data protection measures, data retention and data disposal requirements were not defined and implemented.

Root Cause and Impact

IT management was aware of the deficiency but did not take any measures due to limited IT resources.

Without a formal DG framework, critical and sensitive data may not be adequately protected resulting in data loss or breach.

Recommendation

A DG framework that defines data ownership, data classification, data retention and data disposal requirements should be established. Controls

> should be implemented to ensure critical and sensitive data is adequately protected. (Emphasis added)

[138] These strike me as important findings that identify significant deficiencies in CRR's security controls at the time of the audit. The AGCO Audit Report classifies both findings as having a risk rating of "medium," which is defined in the report as follows:

Medium	There is a moderate probability that the finding will have an adverse effect on game integrity, honesty, public interest and minimizing unlawful activity, if unresolved. The finding requires attention by senior management and should be addressed within 6 – 12 months.

[139] The CRR Audit Response outlines CRR management's response to the findings and recommendations of the AGCO Audit Report. With respect to the findings described above (19 and 20), CRR management made the following general comment:

> It is our understanding that the findings in this section of the Audit Report are directly attributable to complying with the new AGCO Registrar's Standards for Gaming which has not yet been implemented and hence, are not a compliance concern. It is respectfully proposed that the findings and recommendations that pertain to complying with the new Standards, be removed from this document, and perhaps placed in a separate document pertaining to recommendations regarding same.

[140] I find this to be a remarkable comment. The AGCO Audit Report specifically notes control deficiencies that put CRR at risk of not only not meeting regulatory requirements of *FIPPA* but potentially resulting in a data breach and, in response to this, CRR's position is that these findings "are not a compliance concern." It is clear from this that CRR did not consider *FIPPA* requirements to be within scope of the AGCO Audit Report.

[141] CRR's timeline for dealing with the findings of the AGCO Audit Report is another important issue to consider. In answer to the follow-up questions regarding audit documentation mentioned above, OLG and CHC submitted:

> The AGCO performed an IT security audit at Casino Rama in 2015. A copy of the AGCO's audit report and Casino Rama's response to the audit report are attached. At that time, the AGCO and CHC agreed that the IT security improvements identified in the course of that audit would be addressed in the course of the implementation of the IT-related Gaming Standards, as discussed in detail in our letter dated August 9, 2017.

[142] In its letter dated August 9, 2017, OLG and CHC described the timeline for implementation of the IT-related Gaming Standards as follows:

> The *Gaming Standards* implementation process at Casino Rama was ongoing at the time of the incident. The AGCO approved a two-phase approach for all of the resort casinos to implement the *Gaming Standards:* first, controls necessary to comply with the non-IT standards were to be implemented by November 30, 2016; and then, controls necessary to comply with the IT standards were to be implemented by April 1, 2017.

[143] This is a considerably longer timeframe than the one proposed in the AGCO Audit Report. As findings with a risk rating of "medium," the AGCO Audit Report proposed a timeline of 6 – 12 months, meaning that the findings would be addressed no later than a year after the release of the report or May 19, 2016. Yet despite this, the AGCO and CHC agreed that the findings would be addressed by April 1, 2017, almost a full year later than initially proposed.

[144] Given this longer timeframe, it is also important to consider the potential effects of the findings in the AGCO Audit Report on the susceptibility of CRR to the cyberattack. In answer to a question regarding the connection, if any, between the findings of the AGCO Audit Report and the occurrence of the cyberattack, OLG submitted:

> None of the risks identified on pages 24 to 32 of the AGCO Audit Report dated May 19, 2015 relate to the susceptibility of the Casino Rama systems to the cyberattack. None of those risks or vulnerabilities were exploited by the cyberattacker in order to gain access to Casino Rama's network and implementation of all of the recommendations made in connection of those risks would not have prevented the cyberattack from occurring. In any event, most of the recommendations in the AGCO audit report had been implemented prior to the cyberattack.

[145] I disagree. A data governance framework is necessary to ensure that an institution's information holdings are classified according to their sensitivity and the potential impact on individuals and the institution in the event that the information is lost, stolen, misused or disclosed inappropriately. Without such an understanding of an institution's information holdings, it is not possible to conduct a threat risk assessment in an appropriate manner to ensure the security of the records at issue. If a data governance framework had been in place prior to the cyberattack, CRR 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 CRR patrons and OLG self-exclusion registrants given its sensitivity, level of risk and the types of threats posed to it. This in turn might have led to stronger security measures being put in place to protect this information in advance of the cyberattack. However, as it stands, CHC did not complete a data governance policy until April 19, 2017, six months after the start of the cyberattack, and when asked to provide copies of all threat risk assessments completed prior to the incident, OLG only provided the Vulnerability Assessment from 2011.

[146] Based on the above, I find that OLG did not have reasonable oversight measures

in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants. Reliance on the regulatory functions of the AGCO is inadequate to ensure compliance with OLG's obligations under the *Act*. While I support OLG's efforts to avoid unnecessary duplication of work with the AGCO, it is clear that the audits of CRR conducted by the AGCO were insufficient for the purposes of the *Act*.

[147] However, since the breach, CHC has addressed the findings in the AGCO Audit Report and has implemented a three-year audit plan as part of its implementation of the Gaming Standards. With respect to the latter, OLG submitted:

> Going forward, either CHC's external or internal auditors will test each of its control activities (including the IT-related control activities) at least once over the three-year period. The result of these audits will be shared with OLG.

[148] I am satisfied with these post-breach measures, although I would recommend in addition that OLG's receipt of the audit results be made a requirement of future operating agreements and include a review to ensure adequate oversight and compliance with its obligations under the *Act*. Requirement 1 of Standard 1.37 of the Gaming Standards provides in particular that "Data collection and protection requirements for player personal information shall meet those set out in the Freedom of Information and Protection of Privacy Act."

CONCLUSION:

1. The information at issue is "personal information" as defined in section 2(1) of the *Act*.

2. The personal information of CRR patrons and OLG self-exclusion registrants was under the control of OLG for the purposes of the *Act*.

3. CRR did not have reasonable measures in place to prevent unauthorized access to the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with section 4(1) of Regulation 460 of the *Act*.

4. OLG did not have reasonable contractual nor reasonable oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants, in accordance with the requirements of the *Act* and its regulations.

RECOMMENDATIONS:

1. Casino Rama IT should include in its phishing awareness communications guidance to the effect that if a CRR employee realizes that they have been

deceived by a phishing email, they should immediately report this to Casino Rama IT.

2. OLG should ensure that future operating agreements incorporate explicit provisions to ensure that the services performed on its behalf comply the rules and safeguards set out in the *Act*.

3. OLG's receipt of audit results under the Gaming Standards should be made a requirement of future operating agreements and include a review to ensure adequate oversight and compliance with its obligations under the *Act*.

4. Within six months of receiving this Report, the OLG should provide this office with proof of compliance with the above recommendations.

[149] The OLG has reviewed this Report and advised this office that Recommendation 1 has been implemented.

Original Signed by: January 30, 2019

Lucy Costa
Investigator