OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Investigation Report F11-01

INVESTIGATION INTO A PRIVACY BREACH OF CUSTOMERS' PERSONAL INFORMATION BY THE BRITISH COLUMBIA LOTTERY CORPORATION

Elizabeth Denham, Information and Privacy Commissioner

February 15, 2011

Quicklaw Cite: [2011] B.C.I.P.C.D. No. 6
CanLII Cite: 2011 BCIPC No. 6
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF11-01.pdf

Summary: The inherent nature and high profile of online gaming websites expose customer personal information to an increased risk. The reasonableness standard in s. 30 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") recognizes that robust security arrangements are required for online platforms, particularly those related to commercial enterprises such as gaming. The Office of the Information and Privacy Commissioner ("OIPC") investigated a July 15, 2010 privacy breach of personal information of British Columbia Lottery Corporation's ("BCLC") PlayNow.com customers and was satisfied that the cause of the privacy breach had been accurately identified and that remediation plans would prevent the privacy breach from reoccurring. Given the security risks of an online gaming website and the fact there had been a privacy breach on the day of the launch, the Information and Privacy Commissioner decided it would be prudent to conduct a second, broader investigation into the general security of the online casino gaming platform to ensure the personal information of PlayNow.com customers was being adequately protected. The cumulative effect of the problems identified in the OIPC's second investigation revealed sufficient security concerns that the Commissioner found BCLC was not in compliance with s. 30 of FIPPA at the time of the launch of the online casino gaming platform of the PlayNow.com website. BCLC has made improvements and now has in place reasonable security arrangements for the protection of the personal information of PlayNow.com customers.

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] On Friday, July 16, 2010, the British Columbia Lottery Corporation ("BCLC") notified the Office of the Information and Privacy Commissioner ("OIPC") that a privacy breach involving the personal information of PlayNow.com customers had occurred the previous day.

[2] The OIPC initiated an investigation of the cause of the privacy breach and the proposed remediation by BCLC. Because of the security risks inherent in an online gaming website and because there had been a privacy breach on the day of the launch of the online casino gaming platform of the PlayNow.com website, I decided it would be prudent to conduct a second, broader investigation regarding the general security of the online casino gaming platform. This report results from my office's two-phase investigation, conducted pursuant to s. 42 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

[3] BCLC is a public body governed under FIPPA and must comply with FIPPA's rules on collection, use and disclosure of personal information; its protection of personal information must meet the standards set in this legislation.

[4] This investigation report is the first time the OIPC has evaluated the security of an online platform and addresses the unique considerations a public body must take into account when making security arrangements in these circumstances. Online platforms have privacy and security risks such as phishing, pharming, malware and spyware that are not common to other systems. Further, online platforms, particularly those related to gaming, attract individuals who make concerted efforts to test the security of a system.

[5] Over the course of this investigation, the OIPC worked closely with the Gaming Policy and Enforcement Branch ("GPEB") of the Ministry of Public Safety and Solicitor General. GPEB regulates all gaming in British Columbia, ensures the integrity of gaming industry companies, people and equipment and provides regulatory oversight of BCLC.

[6] This investigation report does not disclose information that could reasonably lead to a security risk for BCLC's systems. I have specifically noted where such information is withheld.

2.0 INVESTIGATION PROCESS

[7] The OIPC and GPEB engaged Deloitte & Touche LLP ("Deloitte") to assist with the two phases of our investigation. The OIPC also retained a technical advisor to further assist with our investigation.

[8] The OIPC and GPEB set out the terms of Deloitte's work for each phase of the investigation. OIPC investigators participated in regularly scheduled meetings to receive status updates on Deloitte's review and to give further instructions as required.

[9] The OIPC and GPEB conducted a site visit to BCLC during each phase of the investigation to perform an independent verification of select components of security as they relate to the privacy breach and to the online casino gaming platform of PlayNow.com.

[10] The OIPC performed a technical review of the reports from Deloitte for each phase of the investigation and also requested and reviewed further materials and information from BCLC.

3.0 PRIVACY BREACH INVESTIGATION

[11] 3.1 Background

Overview of BCLC and PlayNow.com

[12] BCLC was incorporated in 1984 and operates as a Crown corporation under the *Gaming Control Act*. On behalf of the Government of British Columbia, BCLC conducts, manages and operates:

- Lottery gaming, including marketing nationwide and regional lottery games with other Canadian provinces;
- Casino gaming;
- Community gaming; and
- eGaming.

[13] In 2004, BCLC started the PlayNow.com gaming website with its first game (Sports Action). Since that time, various other games have been added to PlayNow.com.

[14] In 2009, BCLC received ministerial approval to add casino-style games to PlayNow.com. With the July 15, 2010 launch of the online casino gaming platform of the PlayNow.com website, the Government of British Columbia became the first government in North America to offer legal, online casino games. PlayNow.com is open exclusively to residents of British Columbia.

Details of the Privacy Breach of PlayNow.com

[15] BCLC became aware of the privacy breach on July 15, 2010, when various individuals phoned customer service and reported that they were able to view the personal information of other customers when they logged into their PlayNow.com accounts. The first of these phone calls was received by BCLC at 4:17 p.m. After a preliminary investigation, BCLC shut down the PlayNow.com website at 6:18 p.m. The privacy breach and the shutdown of the website occurred on the same day as the launch of the online casino gaming platform of PlayNow.com.

[16] In consultation with the OIPC, BCLC agreed that it would not reactivate the PlayNow.com website until an independent review by this office had been conducted and I was satisfied that the cause of the breach had been identified and effective remediation plans were in place.

[17] In response to the privacy breach, BCLC conducted an internal investigation and identified the cause of the breach as a "data crossover" caused by a default configuration setting within the computer server environment. The effect was that under certain conditions, including high customer traffic, the "data crossover" caused some customers to be switched to the accounts of other customers.

[18] BCLC discovered that the problem could be remediated by altering the configuration setting. BCLC performed additional testing, which confirmed that the proposed change remediated the issue.

[19] BCLC also reviewed the information each of its PlayNow.com customers had been able to view during the time they were logged into their accounts. BCLC's investigation revealed that 134 PlayNow.com customers' personal information could potentially have been viewed by 105 other customers of PlayNow.com. Of these 134 customers, BCLC was able to verify that 18 actually had their personal information viewed by someone else.

[20] The personal information that was compromised included:

- Contact information – name, gender, email address, phone number and address;
- Credit card information – the first digit and last four digits, expiry date, name on card, card type;
- Bank account information – account holder name, transit number, institution number, account number; and
- Account settings – secret questions and answers.

[21] BCLC took steps to ensure that no PlayNow.com customers suffered any financial loss as a result of other customer's gambling from their accounts because of the "data crossover".

Deloitte's Review of the Privacy Breach

[22] On behalf of the OIPC and GPEB, Deloitte was engaged to conduct a review of the cause of the privacy breach and proposed remediation by BCLC.

[23] Deloitte was instructed by the OIPC and GPEB to assess and confirm the root cause of the "data crossover" and the effect of BCLC's remediation plans.

[24] After conducting its review, Deloitte submitted a report to the OIPC and GPEB on August 17, 2010 entitled, *PlayNow.com incident and remediation review*, which concluded:

> Deloitte is confident that the root cause identified by BCLC did cause the data crossover issue and that the remediation plans developed and implemented by BCLC, effectively remediates the root cause.

[25] The August 17, 2010 Deloitte report has not been attached to this report as it contains large amounts of information that could reasonably lead to a security risk for BCLC's systems.

[26] **3.2 Discussion**—Section 30 of FIPPA requires public bodies to make reasonable security arrangements to protect personal information in their custody or under their control. It reads as follows:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[27] "Personal information" is defined in FIPPA as:

> **"personal information"** means recorded information about an identifiable individual other than contact information.[1]

Issue

[28] Did BCLC take reasonable steps in responding to the July 15, 2010 privacy breach?

The Standard of Reasonableness

[29] In Investigation Report F06-01, former Commissioner David Loukidelis interpreted the standard of reasonableness as set out in s. 30 of FIPPA in his investigation into the sale of provincial government computer tapes containing personal information.[2] Commissioner Loukidelis stated:

> ***What does "reasonableness" mean?***
>
> [49] By imposing a reasonableness standard in s.30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is

[1] FIPPA, Schedule 1, also defines "contact information" as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual."
[2] http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf.

> not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
>
> [50] The reasonableness standard in s.30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

The Standard of Reasonableness for an Online Platform

[30] Online platforms have privacy and security risks such as phishing[3], pharming[4], malware[5] and spyware[6] that are not common to other systems. The typical customer of an online gaming website does not have a thorough understanding of these risks nor do they know how to adequately protect themselves from these risks.

[31] The inherent nature and high profile of online gaming websites expose customer personal information to an increased risk. Gambling attracts the attention of organized crime and these individuals or groups have the means and the inclination to test the security of online gaming platforms.

[32] Another consideration in determining the appropriate standard of reasonableness is that BCLC is a Crown corporation of the Government of British Columbia. Government's involvement in online gaming results in an increased level of trust and confidence by customers in the security measures that have been put in place to protect personal information. With this increased level of trust comes a corresponding increase in responsibility.

---

[3] "Phishing" is the practice of creating mirror websites and then sending emails to customers to ask them to update their records at a fake link, resulting in the customer providing personal information. Phishing sites are often extremely sophisticated and difficult to distinguish from real sites.

[4] "Pharming" involves the malicious tampering with a domain name with the result that a customer or potential customer can type in a URL and be redirected to a compromised site without knowledge of the change.

[5] "Malware" is short for "malicious software" and describes software that causes damage to a single computer, server or computer network through a variety of means.

[6] "Spyware" is software that obtains information from a user's computer without that person's knowledge or consent.

[33] It is important to remember that the online environment is one of constant change. As a result, public bodies must respond quickly to any identified privacy and security risks. Failure to do so will be considered unreasonable. However, reasonableness goes beyond simply responding to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their online platforms. Public bodies must also ensure their policies are up to date and that their staff receives regular training.

[34] While "reasonable" does not mean perfect within the context of s. 30 of FIPPA, "reasonable" does require a high level of diligence where a public body chooses to do business in the online world. Given the additional security risks of an online gaming platform, a very high level of rigour is necessary when considering the reasonableness of such security measures. The OIPC has applied this standard in our review and evaluation of BCLC's actions in response to the privacy breach.

What is a Privacy Breach?

[35] A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information that is in the custody of or under the control of a public body. Such activity is "unauthorized" if it occurs contrary to the provisions of FIPPA.

The Privacy Breach Response

[36] In order to help public bodies and private sector organizations evaluate their compliance with the FIPPA security standard, the OIPC has published a document setting out the four key steps for managing a privacy breach.[7] Where a privacy breach occurs, public bodies need to make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring.

[37] The four key steps that public bodies must undertake in managing a privacy breach are:

1. Contain the breach;
2. Assess the risk of harm;
3. Determine whether notification is required; and
4. Develop prevention strategies.

[7]The OIPC has produced a document entitled, "Key Steps in Responding to Privacy Breaches" available at: http://www.oipc.bc.ca/images/stories/pdfs/Policy/Key_Steps_Privacy_Breaches%28June2008%29.pdf .

[38] For the greatest effect, the first three steps should be taken simultaneously or in quick succession.

Contain the Breach

[39] On Thursday, July 15, 2010, various individuals phoned BCLC's customer service and reported that they were able to view the personal information of other customers when they logged into their PlayNow.com accounts. After investigating these phone calls, BCLC shut down the PlayNow.com website two hours after the first call was received. These were appropriate steps to take in the circumstances and effectively contained the breach once discovered.

Risk Assessment

[40] In order to determine what additional steps are immediately necessary, public bodies are expected to evaluate the risks associated with the breach.

[41] In this case, the personal information was very sensitive. Given the nature of gambling websites, the prospect of criminal activity or other intentional wrongdoing is considerable. The personal information at risk in this case included:

- Contact information;
- Credit card information;
- Bank account information; and
- Account settings – secret questions and answers.

[42] The OIPC investigation revealed that BCLC was relying on a service provider to notify them of system vulnerabilities such as the one that caused the privacy breach. Although the vulnerability had been identified in some versions of the software, it had not been identified as an issue in the version that was in use at BCLC. Delays in the vulnerability assessment and notification process resulted in BCLC not being notified in a timely manner of the system vulnerability that caused the privacy breach. As of the date of the privacy breach, the software vendor had not released a patch to address the vulnerability.

[43] BCLC assessed the risks from the privacy breach to those affected as identity theft and potential fraud. BCLC agreed to pay for a credit monitoring service for the customers who had sensitive personal information viewed by others to ensure these individuals were not affected by any resulting fraudulent activity. No customers reported any resulting problems to BCLC.

[44] I find that BCLC correctly considered the risk of potential harm to those affected, concluded that notification was required and undertook preventative measures to ensure that a future similar "data crossover" could not occur.

Notification

[45] Giving notice to affected individuals is often the most important step in responding to a privacy breach. While various individuals or groups may require notification after a privacy breach, the most important of these are the affected individuals.

[46] In Investigation Report F07-01, Commissioner Loukidelis stated "The reasonableness of timing is measured by whether it is objectively diligent and prudent in all the circumstances." [8] In the online world, where the opportunity to exploit privacy breaches is greatly increased, as are the consequences to those affected, timeliness is measured in hours, not days. Providing adequate notification allows individuals to effectively mitigate any harm they may suffer and also provides the opportunity for individuals to make an informed decision as to whether they wish to continue using the online service.

[47] The OIPC discussed notification of affected individuals with BCLC after BCLC reported the privacy breach. Subsequently, BCLC contacted the 18 individuals affected by the breach by telephone on Monday, July 19, 2010 and Tuesday, July 20, 2010. These 18 individuals as well the 105 individuals who had potentially viewed the personal information of others were contacted by BCLC by email between Friday, July 30, 2010 and Tuesday, August 3, 2010. BCLC requested that the 105 individuals who had potentially viewed the personal information of others delete any personal information they may have recorded.

[48] I find that BCLC gave effective and timely notification of the privacy breach to those individuals affected.

Prevention Strategies

[49] In order to recommend prevention strategies, it is necessary to understand the cause or causes of the privacy breach. BCLC's internal investigation after the privacy breach identified what it believed to be the cause. BCLC then put in place remediation plans to address this issue. Deloitte concluded that BCLC had properly identified the root cause and that the remediation plans developed and implemented by BCLC effectively remediated the root cause.

[50] Based on the OIPC investigation, including a site visit to BCLC, as well as our own technical review of the Deloitte report and other information provided by BCLC, I am satisfied that the cause of the privacy breach was correctly identified and that the remediation plans developed and implemented by BCLC will prevent this technical problem from occurring again.

---

[8] [2007] B.C.I.P.C.D. No. 1.

[51] **3.3 Conclusion – Breach Investigation**—I find that BCLC took reasonable steps in responding to the privacy breach and in so doing complied with s. 30 of FIPPA. In summary, I find:

1. BCLC's initial breach containment steps were appropriate in the circumstances and effectively contained the breach once discovered.

2. BCLC correctly considered the risk of potential harm to those affected.

3. BCLC gave effective and timely notification of the privacy breach to those individuals affected.

4. BCLC identified the cause of the privacy breach and put in place effective remediation plans to prevent the breach from occurring again.

[52] The cause of the privacy breach was not one that BCLC could reasonably have prevented because the vulnerability that caused the breach had not yet been identified by BCLC's service provider as applying to the version of the software in use at BCLC. However, given the security risks inherent in an online gaming website and the fact there had been a privacy breach on the day of the launch, I decided a more thorough investigation of the general security of the online casino gaming platform was necessary to ensure the personal information of PlayNow.com customers was being adequately protected. As a result, Deloitte was commissioned to conduct a second, broader investigation into the security of the online casino gaming platform generally. The results of that investigation are set out below.

4.0 INVESTIGATION INTO ONLINE CASINO GAMING PLATFORM

[53] **4.1 Background**—In the second phase of our investigation, Deloitte was retained by the OIPC and GPEB to review BCLC's security practices surrounding the PlayNow.com online casino gaming platform. The details of this Statement of Work are reflected in the Deloitte report dated January 27, 2011, which is attached to this report.

[54] Deloitte was instructed to focus its review on two specific areas:

- Practices in place at BCLC as part of the pre-launch system development life cycle used for the PlayNow.com casino style games project; and
- Assessing current information systems security practices for the PlayNow.com online casino gaming platform.

In conducting its review, Deloitte was not asked to provide findings concerning BCLC's compliance with applicable legislation.

[55] In a 17-page report submitted to the OIPC and GPEB on January 27, 2011, Deloitte made 15 recommendations as to how BCLC could improve its current practices. In response to the recommendations, BCLC developed a series of action plans. BCLC completed many of its action plans as Deloitte identified issues and has committed to completing all of them by the end of 2011.

[56] **4.2 Discussion**—In this phase of the investigation, I must again look at the reasonableness standard set in s. 30 of FIPPA. For the reasons discussed earlier in this report, while "reasonable" does not mean perfect within the context of s. 30 of FIPPA, I believe that a very high level of rigour is necessary when considering the reasonableness of BCLC's security measures for its online casino gaming platform.

[57] When public bodies choose to conduct business or to deliver services online, citizens expect that their personal information will be adequately protected. The elements of "reasonable security" within the meaning of s. 30 of FIPPA in an online environment include, but are not limited to, constant monitoring and testing of security architecture, processes and procedures in place to respond and adapt immediately to newly identified risks and to reasonably anticipated risks. Time is of the essence in responding to risks in an online environment. Public bodies must constantly educate themselves and their employees about common industry security standards and practices as well as international security standards such as ISO 27001, ISO 27002 and the Payment Card Industry Data Security Standard. A failure in any one of these areas could result in a failure to meet the requirements of s. 30 of FIPPA.

Issues

[58] The issues to be addressed in this phase of the investigation are:

1. Did BCLC have reasonable security arrangements in place for its online casino gaming platform when it was launched on July 15, 2010, as required by s. 30 of FIPPA?

2. Does BCLC currently have reasonable security arrangements in place for its online casino gaming platform, as required by s. 30 of FIPPA?

Deloitte Review of Security Arrangements

[59] In this section, I highlight some of Deloitte's observations, implications and recommendations that are of particular relevance in determining whether or not BCLC had made reasonable security arrangements as required by s. 30 of FIPPA. I have also included a summary of BCLC's corresponding action plans.

Malicious code controls

[60] Deloitte identified two findings to enhance controls already in place to prevent malicious code from infecting the PlayNow.com online casino environment.

[61] As a result of discussions involving the OIPC, GPEB, BCLC and Deloitte, a portion of page 13 of the Deloitte report has been withheld. The release of this information could reasonably be expected to harm the security of the PlayNow.com online casino gaming platform.

Transmission of unencrypted personal information

[62] In order to verify customer identity, BCLC collects personal information from potential customers. Once an account has been created, BCLC collects payment information from customers. As part of the registration process, a small number of potential customers – specifically, those who fail a standard screening process to verify their identity as they are trying to register – are asked to email a copy of their credit card statement and driver's license to BCLC for customer verification purposes.[9] Although customers are requested to "black out" very sensitive information (such as their BC driver's license number and credit card number), these documents are transmitted unencrypted by email to BCLC Customer Service.

[63] As email is not a secure communication channel, there is a risk of the email being intercepted during transmission, which could result in inappropriate disclosure of personal information. As such, Deloitte recommends that BCLC establish alternative secure methods for customers to send personal information to BCLC – for example, via fax or a secure upload site. Where customers forward personal information over an unsecure channel, they should be asked to confirm they understand this is occurring.

[64] *BCLC Action Plan*: BCLC will use a new identity verification service that allows agents to verify customers based on verbal responses to questions. BCLC will also implement a secure upload option for customers to submit personal information and will advise customers who wish to send information via email to black out sensitive information.

---

[9] In the course of this investigation, the OIPC identified this portion of the registration process as unnecessary collection by BCLC under FIPPA for the purpose of verifying the identity of PlayNow.com customers. We raised our concerns with BCLC and they have been addressed to our satisfaction.

Information systems security ("ISS") policy

[65] While BCLC's ISS policy contains the components of an accepted international security standard, it has not been formally reviewed since 2005. This results in a risk that BCLC's ISS policy is not updated in response to changes to BCLC's business or technical environment. Deloitte recommends that the ISS policy be reviewed and signed off by BCLC management.

[66] *BCLC Action Plan*: A review and sign-off of the ISS policy has been completed. Going forward, the policy will be reviewed and updated in accordance with the schedule within the BCLC policy framework.

ISS training

[67] ISS awareness sessions were delivered to employees and service providers involved in PlayNow.com. However, the individuals who attended the sessions were not formally tracked. A number of individuals were identified on the PlayNow.com production system who had not attended an ISS awareness session. These individuals run an increased risk of taking actions that are contrary to BCLC's established ISS policies and procedures. Deloitte recommends that all eGaming information technology staff and contractors complete the training.

[68] *BCLC Action Plan*: All eGaming information technology staff and contractors have now completed ISS training. As well, BCLC management has implemented a program that will automatically track individuals who have completed the training.

Media disposal and tracking procedure

[69] No documented media disposal and tracking certification procedure is currently in place. Hard drives that require decommissioning are sent to BCLC's Vancouver office for incineration; however, there is no certification issued once the media have been destroyed. Current practice results in an increased risk that media containing sensitive information is not adequately disposed of, as there is no formal record of the media having been destroyed. Deloitte recommends that media disposal and tracking certification procedures be formally documented and approved and that a process be introduced to certify that media has been destroyed.

[70] *BCLC Action Plan*: BCLC will update its security policy for media destruction to include certification as well as tracking that the media have been destroyed.

Third-party contracts

[71] The third-party contracts with the application service providers do not require the service providers to adhere to BCLC ISS policies and procedures, including privacy requirements. This increases the risk that service providers take action that violates BCLC's policies and procedures. Deloitte recommends that BCLC amend the contracts to include a clause requiring service provider personnel to adhere to BCLC ISS policies and procedures, including privacy requirements.

[72] *BCLC Action Plan*: BCLC will negotiate a new privacy and information security protection schedule with its service providers for inclusion into their contracts with BCLC.

Access to Production

[73] A small number of users' accounts were found on the PlayNow.com production systems where those users no longer required access. One of these users had accounts on the production, development, quality assurance and staging environments, resulting in a lack of separation of duties. This increases the risk of changes being made to the production environment that are not in line with management's intentions. Deloitte recommends that BCLC implement a process to periodically review all users with access to the production environment to ensure access is appropriately restricted.

[74] *BCLC Action Plan*: BCLC reviewed and verified all production accounts on PlayNow.com. It will continue to review monthly.

Patch Management

[75] When Deloitte conducted its review, it discovered that BCLC had not introduced patches since the PlayNow.com environment was "frozen" in June 2010 during the launch of the online casino games (the post-implementation plan of BCLC was to re-introduce regular patching about six to eight weeks post-launch) – contravening BCLC policy and good practice. Applying system patches in a timely manner helps to maintain the security and integrity of the systems. Deloitte recommends that BCLC reassess and, where appropriate, apply the patches released since June 2010.

[76] *BCLC Action Plan*: BCLC has reviewed all patches and developed a testing and implementation plan. BCLC has updated all patches as a result of this review.

Did BCLC have Reasonable Security Arrangements at the Time of the Launch of the Online Casino Gaming Platform?

[77] After reviewing the Deloitte report evaluating the security arrangements in place for the PlayNow.com online casino gaming platform, conducting a site visit to BCLC and performing an independent verification of select security components, I find that the security of the online casino gaming platform was not reasonable within the meaning of s. 30 of FIPPA at the time of the launch for the following reasons:

1. BCLC's malicious code controls did not meet industry best practice standards;
2. User access to the production environment was not appropriately restricted;
3. BCLC did not have adequate processes in place to ensure system patches were applied in a timely manner to help maintain the security and integrity of the systems;
4. BCLC had in place an inadequate tracking procedure for media disposal;
5. Some customers of PlayNow.com were required to transmit personal information using unencrypted data transmissions; and
6. There were inadequate privacy management framework structures in place (including policies, training and third-party contracts).

[78] I do not find there to be any single deficiency in BCLC's security arrangements at the time of the launch that, on its own, would support a finding that BCLC has contravened s. 30 of FIPPA. However, the cumulative effect of the problems that have been identified amount to a sufficient deficiency in the level of security that I find BCLC's security arrangements were not reasonable within the meaning of s. 30 of FIPPA at the time of the launch.

[79] In many instances, BCLC took steps to immediately resolve security issues identified by Deloitte. To date, BCLC has taken the following steps to secure the PlayNow.com platform:

- BCLC has enhanced its project assurance framework to better align with industry best practices by improving project governance and independent oversight of projects.
- BCLC has put in place quarterly risk updates by the Risk Management Group with all project teams.

- BCLC has completed a review and sign-off of the ISS policy and has committed to scheduled reviews and updates in the future.

- BCLC has provided ISS training to those who had not completed it and are introducing an online security awareness program that will automatically track individuals who have completed training.

- BCLC has updated its security policy for media destruction as well as its procedures to include certification and tracking of media that has been destroyed.

- BCLC has updated its emergency change management procedures to require that shift managers are notified of all emergency changes.

- BCLC has formally documented and approved a policy and procedure to manage encryption keys.

- BCLC has implemented a process to periodically review all users with access to the production environment to ensure access is appropriately restricted.

- BCLC has reviewed all patches and developed a testing and implementation plan. BCLC has updated all patches as a result of this review.

Applying s. 30 of FIPPA Considering BCLC's Remediation to Date

[80] The above-listed areas of remediation have resulted in a marked improvement in the security arrangements of the online casino gaming platform. After reviewing all of the remediation activities completed to date by BCLC, I am satisfied that BCLC has put in place reasonable security arrangements for its online casino gaming platform, as is required by s. 30 of FIPPA.

[81] **4.3 Conclusion – Platform Security**—In looking at the overall security of the online casino gaming platform, I find that:

1. The cumulative effect of the problems that were identified indicate sufficient security concerns that BCLC was not in compliance with s. 30 of FIPPA at the time of the launch of the online casino gaming platform of the PlayNow.com website.

2. BCLC has made significant security improvements in carrying out its action plans. I find that these improvements are sufficient that BCLC now has reasonable security arrangements for the protection of the personal information of PlayNow.com customers, as is required by s. 30 of FIPPA.

[82] While it is not determinative of compliance with s. 30 of FIPPA, I do not believe any of Deloitte's or my above-stated concerns regarding BCLC's security arrangements would have prevented the "data crossover" issue. The "data crossover" was caused by a particular issue that has since been remediated by BCLC. The identified concerns with BCLC's security arrangements did not cause or contribute to the "data crossover". This conclusion was also reached by Deloitte and GPEB.

5.0 PRIVACY MANAGEMENT FRAMEWORK

[83] An effective privacy management framework is essential for public bodies to manage privacy and security issues and ensure reasonable security arrangements are in place on an ongoing basis. A review of a privacy management framework is a holistic consideration of the structures, policies, systems and procedures in place to coordinate privacy work, manage privacy risks and ensure compliance with FIPPA. A privacy management framework reflects privacy principles and best practices and is required by the guidance document of the Canadian Institute of Chartered Accountants, *Generally Accepted Privacy Principles*.[10]

[84] I have been informed by BCLC that it has recently added the responsibility of the Director of Privacy to the role of Senior Legal Counsel. Having in place a dedicated position responsible for privacy measures in the organization is a positive move for BCLC in ensuring that privacy measures are considered upfront in future projects.

[85] In the following paragraphs, I have identified current practices of BCLC that I recommend be changed to reflect privacy principles and best practices:

[86] **5.1 Third-party Contracts**—BCLC has committed to negotiating a privacy and information security protection schedule in each of its agreements with service providers. BCLC must be satisfied that its service providers have policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times.

---

[10] See http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/item10677.pdf.

OIPC Recommendation #1

BCLC should negotiate a standard contract term to have the right to audit and inspect how service providers handle and store personal information, and exercise that right to audit and inspect when warranted.

BCLC Action Plan: BCLC does incorporate a term regarding audit and inspection powers into its contracts with some service providers. BCLC agrees that it should extend these powers to every service provider that has access to personal information. Effective March 1, 2011, BCLC will identify all new contracts to which this recommendation applies.

[87] **5.2 BCLC Policies**—During the OIPC's investigation, we requested the ISS policy from BCLC on numerous occasions but BCLC employees we contacted were initially not sure of its existence or whereabouts. Further, in Deloitte's review it was discovered that various BCLC policies had not been kept current.

OIPC Recommendation #2

The following measures should be put in place by BCLC to ensure effective implementation of policies:

- Provide sufficient resources and time for the initial creation of an effective policy;
- Have a central repository for policies that staff know about and can access at any time; and
- Monitor, assess and adapt privacy policies on an ongoing and as-needed basis.

BCLC Action Plan: BCLC agrees and has measures in place to meet this recommendation.

[88] **5.3 Privacy Impact Assessments ("PIAs")**—A PIA is a critical tool to enable BCLC to properly assess whether a proposed program or policy has any privacy impact or complies with FIPPA. Prior to launch of the online casino gaming platform, BCLC completed an undated PIA regarding the implementation of the online casino gaming platform.

[89] In the PIA, BCLC accurately identified the major privacy risk as a privacy breach where personal information could be used for identity theft or fraud. BCLC stated in the PIA they would manage this risk by:

- Providing access to BCLC employees on a need-to-know basis;
- Providing privacy training to BCLC employees as part of the privacy program;
- Reviewing contracts with service providers and amending if necessary; and
- Security – [ensure proper use of] encryption.

[90] With the exception of providing privacy training to employees, BCLC did not adequately mitigate these identified risks until this investigation took place.

OIPC Recommendation #3

BCLC should complete a PIA, in consultation with its privacy experts, at the earliest possible stage for each proposed program or policy. The PIA should be reviewed and updated at the conceptual phase, the design phase and the implementation phase to ensure that the PIA is treated as an evergreen document.

BCLC Action Plan: BCLC agrees with this recommendation and will have measures in place effective March 1, 2011 to ensure this is carried out.

OIPC Recommendation #4

It is not sufficient for a PIA to identify privacy risks and potential strategies to mitigate these risks. Mitigating action has to be taken by BCLC to implement the strategies and this action should be documented in the PIA.

BCLC Action Plan: BCLC agrees and will ensure appropriate measures are in place effective March 1, 2011 to fully implement this recommendation.

[91] **5.4 Records Retention and Disposition Schedules**—The PIA also indicated that BCLC does not have a records retention and disposition schedule in place. As such, it appears that customer personal information is retained

indefinitely. BCLC should not have ongoing access to personal information where individuals have discontinued use of their PlayNow.com account.

OIPC Recommendation #5

BCLC should have a retention and disposition schedule in place that sets out when the disposal of personal information of former customers will occur.

BCLC Action Plan: BCLC is in the process of taking the necessary steps to have retention and disposition schedules in place.

6.0 CONCLUSION

[92] The OIPC investigation regarding the July 15, 2010 privacy breach of the personal information of PlayNow.com customers resulted in a finding that BCLC took reasonable steps in responding to the breach and in so doing complied with s. 30 of FIPPA. However, our investigation did lead me to believe a more thorough investigation of the online casino gaming platform was necessary in order to be assured that BCLC was adequately protecting the personal information of its customers.

[93] As a result of the second phase of the OIPC investigation, I find that the cumulative effect of the problems that were identified reveal sufficient security concerns that BCLC was not in compliance with s. 30 of FIPPA at the time of the July 15, 2010 launch of the online casino gaming platform of the PlayNow.com website.

[94] Keeping in mind that "reasonable" does not mean perfect within the context of s. 30 of FIPPA, I find that BCLC has made sufficient improvements to date that it now has in place reasonable security arrangements for the protection of the personal information of PlayNow.com customers, as is required by s. 30 of FIPPA.

[95] BCLC has committed to the completion of actions plans by the end of 2011 for the OIPC recommendations as well as the remainder of the Deloitte recommendations. The OIPC and GPEB will be monitoring BCLC to ensure we are satisfied that BCLC has carried out its action plans.

[96] It is critical that BCLC is proactive in dealing with the challenges it faces in maintaining reasonable security arrangements for the protection of its customers' personal information. The reasonableness standard in s. 30 of FIPPA recognizes that, because the online world is one of constant change, the

measures needed to protect personal information are also constantly evolving. As such, BCLC needs to ensure that there is an ongoing review of security arrangements and standards, policies and procedures and that the training of staff is kept current.

7.0 ACKNOWLEDGEMENTS

[97] I would like to thank GPEB, with whom my office will continue to work on this matter as we monitor the progress of BCLC's action plans.

[98] Under the direction of Michael Graydon, President and Chief Executive Officer, and his colleagues, BCLC cooperated fully with our work.

[99] Patrick Egan, Senior Investigator, and Troy Taillefer, Policy Analyst, co-ordinated this investigation and prepared this report.

February 15, 2011

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File: F10-42797