

ALBERTA

**OFFICE OF THE INFORMATION AND PRIVACY
COMMISSIONER**

ORDER P2006-011

February 15, 2008

**PENNY LANE ENTERTAINMENT LTD.
PENNY LANE ENTERTAINMENT GROUP
TANTRA NIGHT CLUB INC.**

Case File Number P0256

Office URL: www.oipc.ab.ca

Summary: The Complainant made a complaint under the *Personal Information Protection Act* (the Act) that an employee of Tantra Nightclub had scanned his driver's license information into a database without his consent when he entered.

The Commissioner found that the Organization did not have a reasonable purpose when it collected the Complainant's driver's license information. In addition, the Commissioner found that the Organization did not have a reasonable purpose for retaining the driver's license information of patrons. As a result, the Commissioner found that the collection of the Complainant's personal information, and that of other patrons, was in violation of sections 7, 8, 13, and 14 of the Act. The Commissioner found that the Organization had not taken reasonable steps to secure the Complainant's personal information under section 34, and had contravened section 35 when it retained the Complainant's driver's license information.

Statutes Cited: AB: *Personal Information Protection Act* S.A. 2003, c. P-6.5 ss. 1, 2, 5, 7, 8, 11, 13, 14, 16, 17, 19, 20, 34, 35

Authorities Cited: AB: Order P2006-008

I. BACKGROUND

[para 1] On August 11, 2005, the Complainant complained to the Commissioner that Tantra Nightclub Inc. (the Organization) in Calgary had scanned his driver's license into a nightclub security system controlled by a third party without his consent and retained the scanned copy when he entered the premises in March 2005.

[para 2] Mediation was authorized, but did not resolve the issue. The matter was originally set down for an oral inquiry, but, with the agreement of the parties, was conducted as a written inquiry.

[para 3] Secureclub Corporation (the Affected Party), which maintains and operates the bar scanning equipment and database of information obtained from scanned driver's licenses, was identified as an affected party and was provided with notice of the inquiry and invited to make submissions.

[para 4] The Applicant and the Organization provided initial written submissions. The Organization also provided rebuttal submissions. The Affected Party did not provide submissions.

[para 5] I began the inquiry on November 23, 2006. On December 11, 2006, I advised the Organization that its submissions and evidence were deficient in areas where it had the burden of proof. The Organization provided further submissions in response to my letter and I concluded the inquiry on February 6, 2007.

II. RECORDS AT ISSUE

[para 6] As this inquiry relates to a complaint about the collection, use and disclosure of personal information, there are no records at issue.

III. ISSUES

Issue A: Did the Organization collect, use and disclose the Complainant's personal information for purposes that are reasonable, as required by section 11(1), 16(1) and 19(1) of the Act?

Issue B: Did the Organization collect, use and disclose the Complainant's personal information only to the extent that is reasonable for meeting the purposes for which the information was collected, used and disclosed, as provided by sections 11(2), 16(2) and 19(2) of the Act?

Issue C: Did the Organization have the authority to collect, use and disclose the Complainant's personal information without consent, as provided by sections 14, 17, and 20 of the Act?

Issue D: If the Organization did not have the authority to collect, use and disclose the Complainant’s personal information without consent, was the Organization(s) required to obtain the Complainant’s consent before collecting, using, and disclosing the Complainant’s personal information, as provided by sections 7(1), 8(2) and 8(3) of the Act?

Issue E: Did the Organization, as a condition of supplying a product or service, require the Complainant to consent to the collection, use or disclosure of personal information about the Complainant beyond what is necessary to provide the product or service, contrary to section 7(2) of the Act?

Issue F: Did the Organization engage the services of a person for the purposes of sections 5(2) and 5(6) of the Act?

Issue G: Was the Organization required to provide notification before collecting the Complainant’s personal information, as provided by section 13 of the Act?

Issue H: Did the Organization protect the Complainant’s personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction, as provided by section 34 of the Act?

Issue I: Is the Organization permitted for legal or business purposes to retain the Complainant’s personal information for as long as is reasonable, as provided by section 35 of the Act?

IV. DISCUSSION OF ISSUES

Preliminary Issues:

Who is the Organization for the purpose of this Inquiry?

[para 7] Tantra Nightclub Inc. (“Tantra”) is registered in the Alberta Corporation Registration System as an Alberta corporation. Since Tantra is a corporation, Tantra is an “organization” as provided by section 1(i)(i) of the Act.

[para 8] Penny Lane Entertainment Ltd. is registered in the Alberta Corporate Registration System as an Alberta corporation. The principle shareholder of Tantra is also shown as owning 100% of the voting shares of Penny Lane Entertainment Limited. Since Penny Lane Entertainment Limited is a corporation, it is also an “organization” as provided by section 1(i)(i) of the Act.

[para 9] Penny Lane Entertainment Group (PLEG) does not appear in the Alberta Corporate Registration System as a corporation, a partnership or a trade name. It is also

not a trade union, and I have no evidence that it is an individual acting in a commercial capacity.

[para 10] In Orders F2006-003/P2006-003, I accepted that persons who were joined for a common purpose were an “unincorporated association” and therefore an “organization”, as provided by section 1(i)(ii) of the Act.

[para 11] PLEG advertises itself as an operator of entertainment and dining venues. PLEG and Penny Lane Entertainment Limited both say that they operate Tantra. The same person is the controlling shareholder of Penny Lane and Tantra.

[para 12] On these facts, I find that PLEG, which is a “group”, is composed of persons (Penny Lane Entertainment Limited and Tantra, at the very least) who are joined for a common purpose. The common purpose in the broad sense is the operation of entertainment and dining venues, such as Tantra. Drivers’ licence information of patrons is uploaded into a database that is accessible to Tantra and other establishments operated by PLEG and Penny Lane Entertainment Limited. Consequently, the common purpose, in the narrow sense that is particularly relevant to this case, is the operation of a database that is accessible to the Organizations’ establishments. I find that PLEG is an unincorporated association and therefore an organization, as provided by section 1(i)(ii) of the Act.

[para 13] Consequently, when I refer to “the Organization” in this decision, I am referring to PLEG, Penny Lane Entertainment Limited and Tantra. However, when I make the Order, I will refer to each organization individually.

Evidence and the Burden of Proof

[para 14] As noted above, I advised the Organization on December 11, 2006 that its evidence and submissions were deficient in areas where it bore the burden of proof. Counsel for the Organization provided further arguments and later submitted the affidavit of an employee of Alpine Computer Solutions. The Organization also argues that the Complainant has not met the burden of proof as the Complainant has not submitted sworn evidence.

[para 15] As there is uncertainty as to who has the burden of proof and what constitutes evidence, I decided to review these requirements prior to analyzing the issues.

[para 16] In Order P2006-008 I said:

In R v. Stone [1999] 2 S.C.R. 290, the Supreme Court of Canada cited Sopinka, Lederman and Bryant, *The Law of Evidence in Canada* which contrasted the evidential burden with the legal or persuasive burden as follows:

The significance of the evidential burden arises when there is a question as to which party has the right or the obligation to begin adducing evidence. It also arises when there is a question as to whether sufficient evidence has been adduced to raise an issue for determination by the trier of fact. The legal burden of proof normally arises after the evidence has been completed

and the question is whether the trier of fact has been persuaded with respect to the issue or case to the civil or criminal standard of proof. The legal burden, however, ordinarily arises after a party has first satisfied an evidential burden in relation to that fact or issue.

The *Personal Information Protection Act* (“PIPA”) like the *Freedom of Information and Protection of Privacy Act* (the “FOIP Act”) is silent with regard to where the burden of proof rests for an inquiry into a complaint about the collection, use and disclosure of personal information. In Order P2005-001, I adopted the approach previously taken in Order 97-004 with regard to the FOIP Act that addressed the burden of proof issue and applied the following criteria:

- a) who raised the issue; and
- b) who is in the best position to meet the burden of proof

Relying on these criteria in Order P2005-001, I stated that a complainant has to have some knowledge of the basis of the complaint and it made sense to me that the initial burden of proof can, in most instances, be said to rest with the complainant. An organization then has the burden to show that it has authority under the Act to collect, use and disclose the personal information.

This initial burden is what has been termed the “evidential burden”. As I have said, it will be up to a complainant to adduce some evidence that personal information has been collected, used or disclosed. A complainant must also adduce some evidence about the manner in which the collection, use or disclosure has been or is occurring, in order to raise the issue of whether the collection, use or disclosure is in compliance with the Act...

As stated in by the Supreme Court of Canada in *R. v. Schwartz* [1988] 2 S.C.R. 443 at paragraph 38:

The party with an evidential burden is not required to convince the trier of fact of anything, only to point out evidence which suggests that certain facts existed.

As the Complainant has raised the initial issue as to the reasonableness of the Organization’s collection of personal information, it will be the Organization who will be best placed to demonstrate the reasonableness of such collection and the other issues raised in this inquiry. The Complainant has raised a *prima facie* case. The Organization is far better placed than the Complainant to meet the burden of proof with regard to the issues touching its commercial activities, the authority and reasonableness of its collection of personal information and the security and notification arrangements undertaken...

I do not envision complainants having a legal burden under the Act. The Complainant’s burden ends with having met the evidential burden, as discussed. The Organization then bears the evidential burden to demonstrate that its collection, use and disclosure of information is in accordance with the Act.

I believe that the Organization is concerned that I am placing a “reverse onus” on it to prove a negative, that is, to prove that it did not breach the Act. On the contrary, the burden is on an organization to show that it has the authority under the provisions of the Act to collect, use or disclose personal information. This is the same burden of proof that is on a public body under the FOIP Act and a custodian under the *Health Information Act*.

[para 17] In the present case, I find that the Complainant has met the evidential burden. He provided direct evidence that the Organization scanned his driver’s license when he attended Tantra in March 2005. The Organization corroborated his evidence by providing affidavit evidence confirming that it has a practice of collecting and retaining the driver’s license information of patrons.

[para 18] As the Complainant has met the evidential burden, the Organization now bears the burden to demonstrate that its collection and retention of his personal information is in accordance with the Act. The Organization may meet this burden by providing evidence in support of its arguments that it has authority under the Act.

[para 19] “FOIP” Practice Note 10 offers a helpful distinction between evidence and arguments. It explains:

“Evidence” is the material that public bodies must submit in inquiries to establish the facts upon which the Commissioner makes decisions. “Arguments” are the interpretation of the law based on the facts... Public Bodies do not meet the burden of proof if they do not provide evidence to support written or oral arguments made in inquiries. Providing arguments alone is not sufficient. Arguments are not a substitute for evidence. It is also not sufficient to provide the Commissioner with records, and leave it up to the Commissioner to figure out from the records the facts upon which he will base his decisions. The Commissioner requires that persons within the Public Bodies provide evidence by speaking to the contents of records. Affidavit evidence is preferred. Public Bodies that do not provide evidence for inquiries risk having decisions go against them for lack of evidence to support their arguments.

The same holds true for organizations under the Act. Even though a hearing is conducted through written submissions, it is still necessary to provide evidence to support the organization’s position. This can be done by submitting affidavit evidence, or the direct evidence of individuals with first hand knowledge of the issues.

Issue A: Did the Organization collect, use and disclose the Complainant’s personal information for purposes that are reasonable, as required by section 11(1), 16(1) and 19(1) of the Act?

Issue B: Did the Organization collect, use and disclose the Complainant’s personal information only to the extent that is reasonable for meeting the purposes for which the information was collected, used or disclosed, as provided by sections 11(2), 16(2) and 19(2) of the Act?

Collection

[para 20] The Complainant argues that while patron safety is a legitimate issue, the Organization did not collect his information for this purpose. He argues that the Organization keeps the information collected indefinitely, shares it with other bars that use the SecureClub database, and does not scan the information of all patrons entering the premises.

[para 21] The Organization states that it scans information from the front of a driver’s license. Driver’s license information includes an individual’s photograph, driver’s license number, birth date and address. In addition, driver’s licenses contain bar codes with embedded information unique to the individual driver’s license on the front. Driver’s license information is personal information within the meaning of section 1(k) of the Act, which states:

1(k) *“personal information” means information about an identifiable individual;*

[para 22] Section 11 of the Act limits the purposes for which an organization may collect personal information. It states:

11(1) An organization may collect personal information only for purposes that are reasonable.

(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.

[para 23] Section 2 of the Act explains what reasonable means in the context of the Act. It states:

2 Where in this Act anything or any matter

- (a) is described, characterized or referred to as reasonable or unreasonable,*
- or*
- (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,*

the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

[para 24] The Organization entered the affidavit of an employee, a notice to patrons which is now posted in Tantra, and a document entitled “Alberta Roundtable on Violence” into evidence in support of its arguments that its collection of driver’s license information is reasonable.

[para 25] The Organization argues that it collects information from drivers’ licenses to “ensure the life, liberty and security of its patrons”, and that this is a reasonable purpose within the meaning of sections 11(1) of the Act. It also submits that it only collects as much information from patrons as is necessary to achieve this purpose.

[para 26] In its submissions of January 31, 2007, the Organization provided the following argument:

It is submitted that the collection of personal information through the SecureClub ID System (SC) is one component of an overall security system. The SC system as part of the overall comprehensive security system, is intended to act as a deterrent to potential wrongdoers in that all patrons know that their identification is scanned and that therefore they could easily be identified if they were involved in any violent or illegal activity. It is submitted that potential wrongdoers would be less likely to engage in violent or other illegal behaviour if their ability to remain anonymous was removed. It is further submitted that the SC system removes the anonymity of

potential wrongdoers, and is therefore one effective component of an effective overall comprehensive security system.

[para 27] The Organization submitted a notice to patrons as an exhibit. This notice advises patrons the following:

The purpose of security systems is to encourage our patrons to behave responsibly and deter those who are seeking to ruin your experience with us, from entering the venue.

[para 28] The affidavit evidence of an employee of the Organization is that by scanning and capturing a patron's identification, the patron can later be identified if they are involved in an incident which threatens the security of another patron.

[para 29] I note that the document entitled *Alberta Roundtable on Violence* contains no reference to the collection of driver's license information as a means to stem violence.

[para 30] Section 11(1) makes it clear that the purpose for collecting personal information must be reasonable. Section 11(2) is equally clear that the collection of personal information must be reasonably related to the purpose for collection. For example, protecting life, liberty, and security of the person may be a reasonable purpose in the abstract, but an organization must also establish that its collection of personal information, in this case, the fronts of driver's licenses, is reasonably related to that purpose to meet the requirements of section 11.

[para 31] From my review of the evidence and the parties' submissions, I find that, at best, the Organization offers conjecture that collecting driver's license information of patrons may act as a deterrent to violent behaviour. The Organization did not submit any evidence to establish that collecting the Complainant's driver's license information, or that of other patrons, is in any way a deterrent to violent behavior. In addition, it did not provide any evidence regarding the causes of violence in bars or statistics relating to the incidence of violence in bars before and after the implementation of a driver's license collection program. I draw the inference that the Organization is unable to produce any evidence to draw a correlation between violence, patron safety, and collecting driver's license information. As a result, the Organization has failed to establish any reasonable relationship between collecting driver's license information and any of its stated purposes for scanning driver's licenses. I am therefore unable to conclude that the Organization has a reasonable purpose within the meaning of section 11 when it scans patrons' driver's licenses.

[para 32] For these reasons, I find that the Organization did not comply with the requirements of either section 11(1) or (2) when it scanned the driver's license information of the Complainant, as its collection of personal information is not reasonable related to its purpose.

Use

[para 33] Section 16 of the Act limits the uses to which an organization may make of personal information. It states:

16(1) An organization may use personal information only for purposes that are reasonable.

(2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.

[para 34] The Complainant's complaint turns on the Organization's collection and retention of his personal information. While he complained that the Organization had also used his information, he provided no evidence to substantiate this aspect of his complaint.

[para 35] The evidence of the Organization is that it uses patron personal information only in situations when a patron is involved in an incident.

[para 36] There is no suggestion that the Complainant has been involved in an incident at Tantra. Consequently there is no evidence to suggest that the Organization has used the Complainant's information.

Disclosure

[para 37] Section 19 of the Act limits the extent to which an organization may disclose personal information. It states:

19(1) An organization may disclose personal information only for purposes that are reasonable.

(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.

[para 38] As noted above, the Complainant's complaint turns on the Organization's collection and retention of his personal information. The Complainant has not provided any evidence that his personal information was disclosed and neither has the Organization.

Issue C: Did the Organization have the authority to collect the Complainant's personal information without consent, as provided by sections 14, 17, and 20 of the Act?

[para 39] As I have found that there is no evidence to suggest that the Organization used or disclosed the Complainant's personal information, I will limit this issue to whether the Organization complied with section 14 when it collected the Complainant's personal information.

[para 40] Section 14 explains when an Organization may collect information without consent. It states:

14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:

- (a) a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;*
- (b) the collection of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the collection;*
- (c) the collection of the information is from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the information to the organization;*
- (d) the collection of the information is reasonable for the purposes of an investigation or a legal proceeding;*
- (e) the information is publicly available;*
- (f) the collection of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;*
- (g) the information is collected by a credit reporting organization to create a credit report where the individual consented to the disclosure to the credit reporting organization by the organization that originally collected the information;*
- (h) the information may be disclosed to the organization without the consent of the individual under section 20;*
- (i) the collection of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;*
- (j) the organization collecting the information is an archival institution and the collection of the information is reasonable for archival purposes or research;*
- (k) the collection of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.*

[para 41] Section 14 must be read in the context of section 11 of the Act. Section 11 allows organizations to collect personal information only for reasonable purposes. As the Organization has not established that it collected the Complainant's driver's license information for a reasonable purpose, the Act prohibits the Organization from collecting that information, with or without the consent of the Complainant.

[para 42] For these reasons, I find that the Organization did not have the authority to collect the Complainant's personal information with or without consent.

Issue D: If the Organization did not have the authority to collect, use or disclose the Complainant’s personal information without consent, was the Organization(s) required to obtain the Complainant’s consent before collecting the Complainant’s personal information, as provided by sections 7(1), 8(2) and 8(3) of the Act?

Issue E: Did the Organization, as a condition of supplying a product or service, require the Complainant to consent to the collection, use or disclosure of personal information about the Complainant beyond what is necessary to provide the product or service, contrary to section 7(2) of the Act?

[para 43] I will consider these issues together. As I have found that there is no evidence that the Organization used or disclosed the Complainant’s personal information, I shall consider these questions only in terms of collection.

[para 44] Section 7 of the Act states:

7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,

- (a) collect that information unless the individual consents to the collection of that information,*
- (b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,*
- (c) use that information unless the individual consents to the use of that information, or*
- (d) disclose that information unless the individual consents to the disclosure of that information.*

(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

(3) An individual may give a consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.

[para 45] Section 7 must also be read within the context of section 11 of the Act. As the Act prohibits collection for unreasonable purposes, it does not matter whether the Complainant consented within the meaning of section 8 to the collection or not: the Organization is prohibited from collecting his driver’s license information if its purpose for collection is unreasonable. The limit section 11(1) places on the collection of personal

information would have no purpose if individuals could consent to the unreasonable collection of personal information under sections 7 and 8.

[para 46] The Organization argues that patrons have the option of providing their driver's license for scanning or not entering Tantra. In other words, it argues that patrons are under no obligation to provide driver's license information to the Organization.

[para 47] However, section 7(2) makes it clear that an individual cannot be required to consent to the collection of information that is unnecessary for the supply of a product or service. In the present case, the Organization collected the Complainant's driver's license information as a condition of entering Tantra. The Organization has not established that collecting all the information on the Complainant's driver's license was necessary to complete the transaction.

[para 48] As I have found that the Organization did not have a reasonable purpose when it scanned the Complainant's driver's license information into a database as a condition of entry, I find that the Organization contravened section 7(2) of the Act.

Issue F: Did the Organization “engage the services of a person” for the purposes of sections 5(2) and 5(6) of the Act?

[para 49] This issue was not raised by the Complainant or the Organization and was apparently added by my office. Neither party provided submissions or evidence in relation to this issue. In addition, I find that answering this question is irrelevant for the determination of this inquiry. As a result, I will not address this issue.

Issue G: Was the Organization required to provide notification before collecting the Complainant's personal information, as provided by section 13 of the Act?

[para 50] Section 13 of the Act explains the notice an Organization must provide prior to collecting personal information. It states in part:

13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally

- (a) as to the purposes for which the information is collected, and*
- (b) of the name of a person who is able to answer on behalf of the organization the individual's questions about the collection.*

(4) Subsection (1) does not apply to the collection of personal information that is carried out pursuant to section 8(2).

[para 51] Section 8(2) explains when an individual is deemed to consent to the collection, use or disclosure of information. It states:

(2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if

- (a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose, and*
- (b) it is reasonable that a person would voluntarily provide that information.*

[para 52] I have already found that the collection of the Complainant's personal information was unreasonable. As discussed above, a Complainant cannot consent to the unreasonable collection of personal information under the Act, or, in other words, an unreasonable collection cannot be ratified by consent.

[para 53] The Complainant's evidence is that his driver's license was scanned before he could raise an objection. He had assumed that the Organization's employee would check his birth date, but she instead scanned the information on the license into a database. The Organization does not challenge the Complainant's version of events, but points to a poster it has now posted for patrons explaining why it collects driver's licenses and what it does with them. It argues that this poster satisfies the requirements of section 13(1).

[para 54] As noted above, the poster explains that its collection practice is intended "to encourage our patrons to behave responsibly and deter those who are seeking to ruin your experience with us, from entering the venue." The poster is not clear about the purposes of the Organization in collecting the information and does not warn patrons that information will be retained for a period of 7 – 10 days or longer by the Organization.

[para 55] I find that the poster is misleading and does not provide sufficient information for patrons to provide informed consent to the Organization's collection of personal information. In addition, the Organization provided no evidence that the poster was in place when it scanned the Complainant's driver's license. In fact, paragraph 8 of the Organization's affidavit establishes only that the notice was posted on August 24, 2006, the date of the affidavit.

[para 56] I find that the Complainant did not consent to the scanning of the information on the face of his driver's license, other than to permit the Organization employee to confirm his date of birth. I also find that the Organization did not provide adequate notice to the Complainant of its collection of his personal information. As none of the provisions of 14 apply, and because an individual cannot consent to the unreasonable collection of personal information, I find that the Organization was required to provide notice of its collection and did not. As a result, I find that the Organization contravened section 13 of the Act when it collected the Complainant's personal information.

Issue H: Did the Organization protect the Complainant’s personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction, as provided by section 34 of the Act?

[para 57] Section 34 of the Act requires an Organization to secure personal information in its custody or under its control. It states:

34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[para 58] The Organization provided a letter from an employee of Alpine Computer Systems. The letter advises:

The Secureclub database has the following security in place:

1. The Database is located on a Microsoft Sql Server which is locked in a secure cabinet.
2. The Sql Server is behind a Cisco PIX Firewall which is commonly used by corporations and government agencies to protect against intrusions from unauthorized personnel.
3. There are logs in place to notify us immediately of any unauthorized personnel accessing data.
4. There are only 2 people with access to the Server, myself, and (another employee).
5. The Server and Firewall are updated on “a regular basis by myself or (another employee).

[para 59] The affidavit evidence of the Organization employee states:

The data created by the SC system is protected from unauthorized use or disclosure through the use of secure passwords, firewalls and audit trails. Any unauthorized access into the database created by the SC system would be immediately identified and corrected. There have been no known breaches of the SC system to date.

[para 60] The evidence of Alpine Computer Systems and the Organization employee confirms that reasonable electronic security measures are in place to protect the database. However, no evidence was provided in relation to the security measures taken to protect information once it has been downloaded from the database by the authorized personnel referred to in the affidavit of the Organization’s employee. Paragraphs 9 and 10 of the affidavit indicate that Organization employees may have access to a unique identifier about individuals when they scan driver’s license information. No evidence was provided as to how the Organization safeguards this information once it is accessed.

[para 61] Finally, the Organization provided no evidence as to the security measures taken to protect the Complainant’s personal information. While it provided general information about database security, it did not provide any evidence that the Complainant’s information is or was actually stored in the database maintained by Alpine

Computer Systems. Had the Organization provided evidence as to when it began using Alpine Computer Systems to maintain its database, I might have been able to infer that the Organization had taken steps to secure the Complainant's personal information. However, no such evidence was provided and I am unable to conclude that the Organization did have appropriate security measures in place at the relevant time.

[para 62] For these reasons, I am unable to find that the Organization has taken reasonable security measures to protect the Complainant's personal information within the meaning of section 34 of the Act.

Issue I: Is the Organization permitted for legal or business purposes to retain the Complainant's personal information for as long as is reasonable, as provided by section 35 of the Act?

[para 63] Section 35 of the Act limits the amount of time an Organization may retain personal information. It states:

35 Notwithstanding that a consent has been withdrawn or varied under section 9, an organization may for legal or business purposes retain personal information as long as is reasonable.

[para 64] The Organization advised in a letter dated July 24, 2007, that it will no longer store the information of patrons whose attendance is without incident indefinitely, but only those who are banned from its clubs. Instead, it will delete the personal information of those who attend without incident from its database within 7 – 10 days.

[para 65] The Organization has provided no rationale for its original practice of retaining driver's license information indefinitely, nor has it provided an explanation of why it requires personal information of clients who are not involved in incidents for 7 – 10 days. In addition, the Organization did not establish that it had a reasonable purpose in retaining the Complainant's personal information for an indefinite period.

[para 66] I have already found that it has no reasonable purpose in collecting or using the information, so it follows that it is not reasonable to retain the information.

[para 67] For these reasons, I find that the Organization retained the Complainant's personal information for longer than was reasonable, contrary to section 35 of the Act.

V. ORDER

[para 68] I make this Order under section 52 of the Act.

[para 69] I order Tantra Nightclub Inc. to destroy the Complainant's personal information that it has in its custody or under its control if it has not already done so.

[para 70] I order Penny Lane Entertainment Group to destroy the Complainant's personal information that it has in its custody or under its control if it has not already done so.

[para 71] I order Penny Lane Entertainment Ltd. to destroy the Complainant's personal information that it has in its custody or under its control if it has not already done so.

[para 72] I order Tantra Nightclub Inc. to cease its practice of scanning the driver's licenses of patrons, as it does not have a reasonable purpose for doing so.

[para 73] I order Penny Lane Entertainment Group to cease its practice of scanning the driver's licenses of patrons, as it does not have a reasonable purpose for doing so.

[para 74] I order Penny Lane Entertainment Inc. to cease its practice of scanning the driver's licenses of patrons, as it does not have a reasonable purpose for doing so.

[para 75] I order Tantra Nightclub Inc. to destroy the information in its custody or under its control that it has gathered by scanning the driver's licenses of patrons.

[para 76] I order Penny Lane Entertainment Group to destroy the information in its custody or under its control that it has gathered by scanning the driver's licenses of patrons.

[para 77] I order Penny Lane Entertainment Inc. to destroy the information in its custody or under its control that it has gathered by scanning the driver's licenses of patrons.

[para 78] I further order Tantra Nightclub Inc. to notify me in writing, within 50 days of its receipt of a copy of this Order, that it has complied with my Order.

[para 79] I further order Penny Lane Entertainment Group to notify me in writing, within 50 days of its receipt of a copy of this Order, that it has complied with my Order.

[para 80] I further order Penny Lane Entertainment Inc. to notify me in writing, within 50 days of its receipt of a copy of this Order, that it has complied with my Order.

Frank Work, Q.C.
Information and Privacy Commissioner