



Office of the Information and
Privacy Commissioner of Alberta

Investigation Report P2021-IR-03

Investigation into Alcanna Inc.'s use of PatronsCan identification-scanning technology

October 6, 2021

Alcanna Inc. and Servall Data Systems Inc.

Investigations 014640 and 014642

Commissioner's Message

Alcanna Inc. (Alcanna) and Servall Data Systems Inc. (Servall) announced on January 20, 2020 the launch of their ID-scanning pilot project at three Edmonton liquor stores that Alcanna operates. During the news conference and in subsequent media interviews, representatives for the organizations repeatedly assured reporters that the technology had been “approved” by my office and the news release stated that “PatronScan technology complies with the Canada, Alberta and BC legislative and regulatory requirements.”

Trouble is, my office first heard about the pilot project on the day it was announced.

Servall relied on a 2009 privacy impact assessment (PIA) review of its technology as evidence that its technology was compliant with the *Personal Information Protection Act* (PIPA). In providing comments to Servall on its 2009 PIA, the first page of the OIPC's response said, “As you know, the OIPC cannot endorse or even approve Servall's product as ‘privacy-compliant’.”

Despite relying on a decade-old review with a disclaimer that says it is not meant as approval, Alcanna and Servall insisted that my office had approved the technology used in the pilot project. When my office confirmed with reporters that we were not aware of the project, the public attention on potential privacy concerns increased.

In addition to the public attention, I joined my federal and British Columbia colleagues in issuing a cease and desist letter to Servall demanding that it immediately stop using our offices' corporate logos and registered trademarks.¹ The logos were displayed prominently on Servall's website. We said, “Your use of the logos creates a misleading and false impression that some or all of your activities are approved by (the Commissioners' offices) when they are not.”

These examples serve as a reminder to all businesses that prior involvement with my office does not give a “seal of approval” for marketing purposes. Additionally, privacy laws are technology neutral. Use of technology depends on context. How technology is implemented, what features are engaged, among several other considerations, substantively affect compliance.

During this investigation, there were 16 findings and five recommendations made to the parties.

Notably, the *Gaming, Liquor and Cannabis Act* (GLCA) provides statutory authority for Alcanna (a licensed premise under the GLCA) to collect name, age and photograph in order to decide whether to grant entry to an individual, in part based on an individual's past involvement in criminal activity.

Alcanna identified two distinct purposes for the collection and use of personal information through the ID-scanning technology: To verify the age of a patron who appears to be a minor, and to identify patrons who have been involved in a prior incident of theft, robbery or violence.

The investigation found that Alcanna's purpose of collecting and using proof of age in order to verify the age of a patron who appears to be a minor is reasonable, as required by sections 11(1) and 16(1) of PIPA. However, it is not reasonable for Alcanna to collect and use personal information for this purpose beyond that which would be viewable on the face of a driver's licence. It is also not reasonable for

¹ Office of the Privacy Commissioner of Canada, [“Letter to Servall Data System \(Patronscan\) on unauthorized use of registered trademarks, corporate logos”](#), January 23, 2020.

Alcanna to retain any information after a decision has been made to grant or deny entry to its premises. To the extent the system collects, uses and retains more than this information for this purpose (for example, when the system collects and retains name, age, gender and partial postal code), Alcanna is in contravention of sections 11(2) and 16(2) of PIPA.

With respect to identifying patrons who have been involved in a prior incident of theft, robbery or violence, the investigation found that the feature meant to “flag” individuals with prior incidents of theft, robbery or violence was not functional in the Alcanna’s stores. Nevertheless, Alcanna’s collection and use of all the information encoded in a driver’s licence barcode, and retention and use of gender and partial postal code, for the purpose of identifying patrons who have been involved in a prior incident of theft, robbery or violence, is beyond the extent reasonable to meet its purpose and is a contravention of sections 11(2) and 16(2) of PIPA.

Another notable finding related to consent. Alcanna’s collection, use and disclosure of name and age without consent for various purposes set out in the GLCA (sections 69.2 and 74) is authorized by PIPA (sections 14, 17 and 20). For example, the GLCA authorizes Alcanna to collect, use and disclose personal information to decide whether or not to allow entry based on past conduct (section 69.2 of the GLCA). Alcanna does not, however, have statutory authority to collect, use or disclose personal information beyond name and age for these purposes. Alcanna is also unable to rely on consent as collection, use or disclosure of personal information beyond name and age for these purposes is unreasonable. PIPA does not allow for the collection of personal information for unreasonable purposes even with consent.

The investigation also found that the personal information collection notice posted in Alcanna’s stores does not comply with section 13(1) of PIPA in that it does not accurately identify the personal information that is collected or the purposes for that collection. It also does not provide the “name or position name or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection”.

Other findings related to safeguards and retention periods.

The following recommendations were made:

- Alcanna cease collecting personal information beyond those information elements specified in the GLCA.
- Alcanna modify the notices posted in its stores to meet requirements under section 13(1) of PIPA.
- Alcanna develop and implement policies and procedures for the Project system if it continues using it, or before it implements it in additional stores.
- Alcanna revise its contract with Servall to address the gaps highlighted in this report, including accountability for personal information collected, used and disclosed as part of the Project, and to clarify the roles of the parties.
- Alcanna consider how long it needs to retain personal information it collects in the Project to reasonably meet its legal and business purposes, and adjust its retention period accordingly.

I appreciate Alcanna and Servall’s commitment to address each of the recommendations.

Jill Clayton
Information and Privacy Commissioner

Table of Contents

- Introduction 8
- Jurisdiction 9
- Issues 10
- Methodology 10
- Background 11
 - The Patronsan System..... 11
- Analysis and Findings..... 13
 - Issue 1: Does Alcanna collect and use personal information only for reasonable purposes, and only to the extent reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA? .. 13
 - Issue 2: Does Alcanna obtain consent for the collection, use and disclosure of personal information, or is the collection, use and disclosure otherwise authorized? 24
 - Issue 3: Does Alcanna notify individuals about its collection of personal information, as required by section 13 of PIPA?..... 28
 - Issue 4: Has Alcanna made reasonable security arrangements to protect Project personal information, as required by section 34 of PIPA?..... 31
 - Issue 5: Does Alcanna comply with section 35 of PIPA for any personal information it retains in relation with the Project? 38
- Summary of Findings..... 40
 - Issue 1 40
 - Issue 2 41
 - Issue 3 41
 - Issue 4 41
 - Issue 5 42
- Summary of Recommendations 42
- Appendix A: Scanning Instructions Poster 43
- Appendix B: Privacy Notice - Poster..... 44
- Appendix C: Privacy Notice - Countertop 45
- Appendix D: Patronsan’s Law Enforcement Agency Information Request Form 46



Introduction

- [1] Alcanna Inc. (Alcanna) operates retail liquor stores in Alberta. On January 20, 2020, Alcanna held a news conference at one of its Edmonton stores to announce the launch of a pilot project (the Project) aimed at addressing an increase in thefts, robberies and violence in its stores.
- [2] According to materials published by Alcanna (see Appendix B), the Project is a partnership between Alcanna and the Edmonton Police Service (EPS) that requires individuals to scan the barcode on the back of their driver's licence as a condition of entering participating liquor stores.
- [3] Alcanna announced it had contracted the services of Calgary-based information technology company Servall Data Systems Inc., which operates as PatronsCan, to provide the technical solution supporting the Project.
- [4] At the time of the news conference, questions were raised by the media about the handling of the personal information of individuals who have their driver's licences scanned. Subsequent media reports quoted Alcanna's CEO as saying that "...the company that developed the scanning system...has 'been working with privacy offices in Alberta, Canada, across North America, to make sure this is all privacy compliant with both laws and norms of society.'".
- [5] ¹
- [6] On January 23, 2020, the Information and Privacy Commissioner (Commissioner) opened an investigation under section 36(1)(a) of PIPA to determine whether Alcanna's use of PatronsCan technology in its liquor stores in Alberta complies with Alberta's *Personal Information Protection Act* of Alberta (PIPA).
- [7] The Commissioner authorized me to conduct the investigation. This report outlines my findings and recommendations.

¹ Rusell, Jennie, "[Alberta privacy commissioner considering investigation of new ID scan system at liquor stores](#)", CBC News, January 22, 2020.

Jurisdiction

- [8] Alcanna is headquartered in Edmonton, Alberta, and operates retail liquor stores in Alberta. Alcanna is incorporated under the *Canada Business Corporations Act* and is an “organization” as defined in section 1(1)(i) of PIPA.
- [9] Servall Data Systems Inc. (Servall) sells and operates its technology solutions in Alberta and other jurisdictions. Servall is headquartered in Calgary, Alberta, and is also incorporated under the *Canada Business Corporations Act*. Servall is an “organization” as defined in section 1(1)(i) of PIPA.
- [10] Patronsca is the name of the identification scanning product developed by Servall. Patronsca is also the operating name for Servall when selling the product. Throughout this report I refer to the organization as “Servall” and the technology system and its components as “Patronsca”.
- [11] Section 5 of PIPA says:
- 5(1) An organization is responsible for personal information that is in its custody or under its control.
- (2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person’s compliance with this Act
- ...
- (6) Nothing in subsection (2) is to be construed so as to relieve any person from that person’s responsibilities or obligations under this Act.
- [12] Alcanna says it has a business relationship with Servall in which “...Servall is a vendor and Alcanna is their customer... Alcanna understands that in accordance with subsection 5(2) of PIPA that Alcanna is responsible for Servall’s compliance with the PIPA.”
- [13] The information at issue in this investigation is information that is encoded in the barcode on an individual’s driver’s licence, and includes, among other things: name, age, gender and first three characters of the postal code. This information is about identifiable individuals and therefore qualifies as “personal information” as defined in PIPA section 1(1)(k).

Issues

- [14] I identified the following issues and notified the Organization that these were the issues I would investigate under PIPA:
- Issue 1: Does Alcanna collect and use personal information only for reasonable purposes, and only to the extent reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA?
 - Issue 2: Does Alcanna obtain consent for the collection, use and disclosure of personal information, or is the collection, use and disclosure otherwise authorized?
 - Issue 3: Does Alcanna notify individuals about its collection of personal information, as required by section 13 of PIPA?
 - Issue 4: Has Alcanna made reasonable security arrangements to protect personal information, as required by section 34 of PIPA?
 - Issue 5: Does Alcanna comply with section 35 of PIPA for any personal information it retains in relation with the Project?

Methodology

- [15] I took the following steps during the course of this investigation:
- Sent Alcanna questions, reviewed their responses and contract with Servall
 - Sent Servall questions, reviewed their responses, sample contract and confirmed the details of how the Patronscan system operates
 - Visited Servall's place of business and interviewed employees
 - Visited an Alcanna store and interviewed store employee and corporate employees
 - Consulted with the Alberta Gaming, Liquor and Cannabis (AGLC)
 - Sent a draft investigation report to the parties for fact checking review, considered feedback and finalized the report accordingly

Background

- [16] Alcanna operates approximately 200 liquor stores in Alberta across several brands, and employed about 1,500 people at the start of this investigation.
- [17] Alcanna says that, between 2017 and 2019, it saw a dramatic increase in the number of thefts from its stores (from 3,588 in 2017 to 11,696 in 2019). Similarly, the number of robberies (theft with violence or threat of violence) increased from 18 in 2017, to 35 in 2019. These numbers are consistent with media reports of liquor thefts², based on EPS statistics.³
- [18] Alcanna says that it has tried several methods to reduce instances of liquor theft, including modified physical store entrance layouts, dedicated personnel (loss prevention and investigation employees), and cooperation with law enforcement.
- [19] The Project is another attempt by Alcanna to curb liquor theft by deterring thieves from entering stores in the first place. Alcanna said the Project could additionally serve to confirm that customers are of legal age at the time they seek to enter any of its stores.
- [20] At the start of this investigation, the Project was running at three Alcanna stores located in Edmonton's northeast; originally, Alcanna suspended implementation at additional stores while the investigation was underway.

The PatronsCan System

- [21] PatronsCan is the system Alcanna has implemented at three of its stores as part of the Project. Servall describes PatronsCan as "...an information system designed to collect, encrypt, store, and retrieve information related to security and public safety matters".
- [22] When individuals seek to enter a participating store, they are required to hold their driver's licence below a scanner located inside a double-door entrance, so the scanner can read the barcode on the back of the driver's licence. If successful, the system unlocks the door to allow the individual to enter the store. Store employees can also unlock the door by pressing a button located at the till.
- [23] Posters on the wall next to the scanner provide instructions to individuals for operating the scanner (see Appendix A).
- [24] The Project system consists of a barcode scanner connected to a small computer⁴ that runs the PatronsCan software. The computer is a processing unit only and there are no connected peripherals (such as monitor, mouse or keyboard) other than the barcode scanner. The computer is in a secure location inside the store and is connected to the internet so that the software can communicate with the PatronsCan data centre and receive updates, and so that

² In this report, "liquor theft" refers to all instances of theft of liquor, whether violent or not.

³ CBC News, "[Edmonton liquor store to combat crime by requiring customers to scan ID before entering](#)", January 20, 2020. This story quotes the EPS as responding to 9,600 liquor theft calls in 2019. Alcanna indicated that law enforcement response is not automatic when liquor theft is reported.

⁴ The computer system runs on a Raspberry Pi®; the computer enclosure is about the size of a wallet.

Servall employees can remotely access the computer to perform software maintenance tasks as needed. Alcanna employees do not have access to the computer.

Analysis and Findings

Issue 1: Does Alcanna collect and use personal information only for reasonable purposes, and only to the extent reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA?

[25] Section 11 of PIPA says:

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.

[26] Sections 16 and 19 of PIPA read the same with respect to the use and disclosure of personal information.

[27] Section 2 of PIPA says:

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.

[28] Alcanna says that it collects the following personal information about individuals when a driver's licence is scanned at a store entrance:

- name,
- age⁵,
- gender, and
- first three characters of postal code⁶.

[29] Alcanna refers to this information as the "Patron Entry Record" and says it collects and uses this information for the following purposes:

Identifying patrons who are involved in a criminal activity that needs to be investigated.

⁵ During the investigation, Alcanna indicated that the computer system was initially set up to collect date of birth in the first few days of the Project, instead of age. It switched to age shortly after this investigation began. For the purpose of this investigation, I have considered the information elements the computer system is currently set up to collect.

⁶ In June 2021, Alcanna indicated that "Servall made the decision in February 2021 to collect only the name and age from an ID". However, this report considers the organization's practices at the time the investigation was underway.

Identifying patrons who have been involved in a prior incident of theft, robbery or violence (“Public Safety Incident”).

[30] Alcanna also says it collects age for the purpose of “Identifying an underage patron”.

[31] I considered each of Alcanna’s stated purposes for collecting, using or disclosing personal information.

To Identify Individuals Who Are Involved in a Criminal Activity That Needs to be Investigated

[32] Alcanna says that one of its purposes for collecting personal information before allowing individuals to enter certain liquor stores is to “[identify] patrons who are involved in a criminal activity that needs to be investigated”. Alcanna also said “...once a robbery is reported, a police officer takes the report and investigates using whatever information from the crime may be available. The Project is an attempt to give more information to identify offenders and then prevent their entry into stores”.

[33] Given this, I understand Alcanna to be saying that it collects personal information before allowing an individual to enter a store, so that the information can be used and disclosed to police in order to identify an individual **after the fact** if the individual is involved in an incident or criminal activity while in the store.

[34] In support of its legal authority to collect personal information, Alcanna says:

Section 69.2 of the Gaming, Liquor and Cannabis Act of Alberta (“GLCA”), does allow for the collection of a person’s name, age and photograph before allowing a person to enter a licensed premises.

[35] With respect to gender and partial postal code specifically, Alcanna says:

The collection of these two extra fields (gender and first three letters of postal code) allow for more accurate identification of the individual in case an incident happens at the Project’s stores. Collecting only name and age makes the system ineffective if an incident were to happen and caused by a person with a common name. For example, properly identifying a 22-year-old John Smith is practically impossible when there are so many people with the name John Smith. Therefore, collection of these extra fields is reasonably required by Alcanna for a reasonable purpose.

[36] Alcanna also says:

Gender is necessary to collect as it helps Servall assisting law enforcement in differentiating individuals between gender neutral names.

[37] I considered Alcanna’s reference to the *Gaming Liquor and Cannabis Act* (GLCA). The GLCA is a statute of Alberta that governs the sale of age-restricted products such as liquor. The GLCA applies to “licensees” in respect of “licensed premises” (defined in subsection 1(p) of the GLCA).

[38] AGLC is responsible to establish and enforce the rules and regulations in Alberta for liquor sale, distribution and consumption, and oversees the GLCA. I confirmed with AGLC that Alcanna is a “licensee” and its stores are “licensed premises” to which the GLCA applies.

[39] I find that Alcanna is a “licensee” subject to the requirements of the GLCA, and its stores are “licensed premises” as that term is defined under the GLCA.

[40] Given this, section 69.2 of the GLCA applies. This section says:

69.2(1) A licensee may, **before allowing a person to enter licensed premises**, collect the person's name, age and photograph.

(2) If a licensee has personal knowledge or reasonably believes that a person referred to in subsection (1) has, at any time within the preceding year, engaged in an activity referred to in section 69(1) or (2), the licensee may, in good faith, disclose the person's name, age and photograph to other licensees for the purpose of allowing them to determine whether they wish to allow the person to enter licensed premises.

(3) **A licensee must, as soon as possible after a request is made by a police officer, disclose to the police officer any information collected under subsection (1).** [emphasis added]

[41] Section 69.2 of the GLCA authorizes a licensee (Alcanna) to collect specific personal information (name, age, photograph) before allowing a person to enter a licensed premise (liquor store).

[42] The GLCA does not specifically state the purpose for which the information may be collected by the licensee, beyond saying "before allowing a person to enter"; however, as the information must be disclosed to a police officer upon request (section 69.2(3)), it is reasonable to assume at least part of the purpose for which the licensee is authorized to collect the information is to be able to assist law enforcement to identify an individual who is involved in an incident or criminal activity in the store.

[43] Given this, I find that it is reasonable for Alcanna to collect some personal information from individuals before allowing them to enter a store in order to "[Identify] patrons who are involved in a criminal activity that needs to be investigated" and reasonable for Alcanna to disclose the information to police on request⁷.

[44] I note, however, that the GLCA specifically authorizes a licensee to collect and disclose name, age and photograph, whereas Alcanna says it collects and discloses name, age, gender, and partial postal code.

[45] As noted previously, with respect to gender and partial postal code, Alcanna says "The collection of these two extra fields (gender and first three letters of postal code) allow for more accurate identification of the individual in case an incident happens at the Project's store s", and "Gender is necessary to collect as it helps Servall assisting law enforcement in differentiating individuals between gender neutral names".

[46] I spoke to Servall about the collection of this information, and the operation of the PatronsCan system generally. Servall described how its software – running on the computers to which the barcode scanners are connected – operates to collect and process the information of individuals. In summary, the process is as follows:

⁷ During the investigation, Alcanna disputed that it is necessary that a purpose be reasonable so long as there is consent, or legal authority to collect personal information without consent. However, this interpretation is incorrect. PIPA says that a collection, use or disclosure of personal information can be "only for purposes that are reasonable", with or without an individual's consent. See [OIPC Order P2006-011](#) at paragraph 41.

Step 1: Retrieval of data stored on driver's licence

- a. When the scanner detects a driver's licence barcode, it retrieves the data on that barcode
- b. Driver's licence data is parsed and data elements are extracted (first name, last name, date of birth, gender, postal code)
- c. These data elements are passed on to the next process, while the remainder of data obtained from driver's licence barcode is discarded

Step 2: Software processes data elements

- a. Data elements are processed:
 - Date of birth is used to calculate an individual's age (based on the date of the day the driver's licence is scanned), and
 - Postal code is truncated to the first three characters
- b. Metadata (such as store identifiers and date / time of scan) are attached to the information

Step 3: Computer uses information and discards local copy

- a. If individual is of legal age, software triggers entrance door to unlock; if the individual is a minor, the entrance door does not unlock and flashes a red light
- b. The Patron Entry Record plus metadata is sent to the PatronsCan data centre over the internet
- a. The copy of the information held in the computer's memory is deleted on successful transmission to the PatronsCan data centre

[47] Servall explained to me that in fact **all** of the personal information that appears on the front of a driver's licence is encoded into the barcode on the back of the same driver's licence, with the exception of the individual's photograph⁸. As a result, when the PatronsCan system scans a barcode on a driver's licence, the PatronsCan software examines **all** the data contained in the barcode including: vehicle class, licence restrictions, licence endorsements, licence expiration date, name, licence issue date, date of birth, gender, eye color, height, address, city, province, postal code, licence identifier, licence number, country, weight, as well as additional technical data specified in the AAMVA DL/ID Card Design Standard⁹.

[48] Although the Project system does not **retain** all of the information contained in the driver's licence barcode, it does initially **decode it**¹⁰ and **process** it (to extract the name, date of birth, gender and postal code; then to calculate the age from date of birth and truncate the postal code). As such, the Project system collects **all** of the personal information contained in the

⁸ Servall pointed out the fact that "While most jurisdictions conform to American Association of Motor Vehicle Administrators (AAMVA) standards, not all do." I confirmed the barcodes on Alberta driver's licences are used to encode the personal information shown on the front of the driver's licence, except for an individual's signature and photograph.

⁹ AAMVA DL/ID Card Design Standard available at <https://www.aamva.org/DL-ID-Card-Design-Standard/>.

¹⁰ The barcode present on the back of driver's licences is a PDF417 barcode that encodes information based on ISO standard 15438. This barcode achieves reliability through embedded error correction. This means that, for a scanning system to decode the information the barcode contains, that system has to scan the entire barcode.

driver's licence barcode, even if most of the personal information collected is only retained for a limited period while it is processed¹¹.

[49] I note that the GLCA (formerly the *Gaming and Liquor Act*) was amended on November 1, 2009 to include section 69.2 authorizing licensees to collect name, age and photograph. In amending the *Gaming and Liquor Act* to allow for the collection of these personal information elements, the Legislature specifically considered what information licensees required in order to decide whether to allow a person entry, and for disclosure to police. The Legislature determined that the personal information elements included name, age and photograph, and not gender and partial postal code, and not every data element contained in the driver's licence barcode.

[50] The AGLC also publishes a "Retail Liquor Store Handbook" (the Handbook) for liquor licensees, including Alcanna. The Handbook includes AGLC policies and guidelines. Section 4.12 of the Handbook speaks to the "Collection of Personal Information", and identifies policies approved in 2012¹². In particular, policy 4.12.1 says that:

Pursuant to Section 69.2(1) of the GLCA, a licensee may, but is not required to, collect a patron's name, age and photograph. **No other information may be collected.** [emphasis added]

[51] I further note that in 2009, the Office of the Information and Privacy Commissioner (OIPC) and the AGLC published *Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons*¹³ (the Guidelines). These Guidelines say:

The *Gaming and Liquor Act* allows licensed premises to collect limited personal information from patrons. **Should a licensee use scanning technology to collect a patron's name, age and photograph, the technology must be programmed to only collect this limited, specific information. Otherwise, it is against the law to scan or photocopy the entire face of a patron's driver's licence or other identification as a condition of allowing them to enter the licensed premises...**[emphasis added]

[52] The Legislature specifically considered what information needs to be disclosed to police in order to identify individuals involved in an incident/criminal activity on licensed premises, and this information is limited to name, age and photograph. The AGLC's policies prohibit licensees from collecting any more information than name, age and photograph pursuant to section 69.2(1) of the GLCA.

[53] As a result, in my view, I find Alcanna's initial collection and use of all the personal information elements encoded in a driver's licence, and retention, use and disclosure of gender and partial postal code thereafter, is beyond the extent reasonable to meet its purpose of identifying individuals involved in criminal activity and contravenes sections 11(2), 16(2) and 19(2) of PIPA.

¹¹ This view is consistent with findings in previous OIPC investigations and orders; a collection occurs when personal information is captured regardless of subsequent uses, accesses, disclosures or retention. See [Investigation Report P2020-IR-01](#) or [Order P2006-008](#).

¹² AGLC updates the Handbook from time to time. In December 2020 section 4.12 was updated to remove a subsection, however that change does not impact the conclusions of this investigation report.

¹³ Office of the Information and Privacy Commissioner of Alberta and Alberta Gaming and Liquor Commission, "[Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons](#)", 2009.

Alcanna and Patronsca n's Responses

[54] On May 11, 2021, I provided Alcanna and Servall with a draft of this investigation report for fact checking. Alcanna and Servall disagreed with my finding above that "the Project system collects **all** of the personal information contained in the driver's licence barcode".

[55] Alcanna stated:

Alcanna strongly disputes that when a barcode is scanned all of that information on the barcode is collected and/or used. Scanning is not collecting. The OIPC did communicate with Servall on this point, however, based on Alcanna's conversation with Servall, Alcanna believes that the process details were misinterpreted by the OIPC and refers the OIPC to [Servall]'s response in this matter; a copy of which is enclosed for reference. When Patronsca n scans the barcode it 'reads' the information but not all of the information is stored and/or used.

[56] Servall stated:

Patronsca n does not "retrieve all" data contained in the barcode. It uses search routines in the barcode and retrieves only the authorized subsets of data. This is analogous to a human examining an ID and retrieving only the authorized subsets of data.

...

As previously stated, Patronsca n "examines" the bar codes and retrieves only authorized subsets of data, it clearly does not "use" all of the data found on the barcode.

...

Our technology uses bar code scanners, magnetic strip scanners and MRZ (machine readable zones found in passports) scanners, all of which include embedded error correction, meaning that the bar code, magnetic strip or MRZ must be examined in its entirety to ensure accuracy.

[57] In addition, in its response Servall cited past cases before the OIPC and said:

This is the same technology that has been investigated multiple times by OIPC of Alberta in the past ... It is important to underscore that the software that Patronsca n uses in nightclubs is the same used in liquor stores. Therefore, it is not logical for the same investigative agency to analyze the same technology more than once, only to find it compliant in one venue and not the other.

[58] I considered the concerns brought forward by Alcanna and Servall. However, I maintain my position and my findings.

[59] First, I note that in previous proceedings before our office, Servall represented, and our office accepted, that its system was only collecting personal information as authorized under the GLCA. In the present investigation, upon close examination of the mechanism through which personal information encoded in the barcode is decoded, I came to a different conclusion regarding the scope of the collection of personal information based on the information provided by Alcanna and Servall.

[60] Then, while both organizations objected to the notion that the Patronsca n system collects all personal information elements encoded in the barcode, Servall confirmed that the Patronsca n system has to decode the personal information embedded in the barcode **as a whole**, in order

to then run predetermined search routines and retrieve certain information elements that are then retained.

- [61] The OIPC's above referenced publication *Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons* states that, "Licensees should remember, however, that 'collection' could include merely examining a patron's identification (e.g. a driver's licence)."
- [62] As such, when the software "examines" the information embedded in the barcode, there is a collection of personal information, including for any personal information that only exists within the PatronsCan software while it is being processed. That processing, which consists in the PatronsCan system running search routines, amounts to a use of personal information.

Findings

- Alcanna is a "licensee" and its retail stores are "licensed premises" as defined in the *Gaming, Liquor and Cannabis Act* (GLCA).
- Section 69.2 of the GLCA authorizes licensees to collect name and age before allowing individuals to enter a store and to use and disclose this information in order to "[Identify] patrons who are involved in a criminal activity that needs to be investigated". This is a reasonable purpose in compliance with sections 11(1), 16(1) and 19(1) of PIPA.
- Alcanna's initial collection and use of all the personal information elements encoded in a driver's licence, and its retention, use and disclosure of gender and partial postal code thereafter, is beyond the extent reasonable to meet its purpose of identifying individuals involved in criminal activity and contravenes sections 11(2), 16(2) and 19(2) of PIPA.

Recommendation

- I recommend that Alcanna cease collecting personal information beyond those information elements specified in the GLCA.

To Identify Individuals Involved in Current or Past Crime

- [63] Alcanna says that another of its purposes for collecting personal information before allowing individuals to enter certain liquor stores is to "Identify patrons who have been involved in a prior incident of theft, robbery or violence".
- [64] Alcanna's written submission for this investigation said the system could serve to flag individuals in relation to an incident, which would cause these individuals to be denied future entry into any of the stores equipped with the PatronsCan system¹⁴.
- [65] Specifically, Alcanna said "The only information that an Alcanna store employee sees, is a coloured light that indicates someone is attempting to enter the store may be underage or

¹⁴ This feature exists in other systems Servall offers for its clients operating bars and nightclubs.

flagged for a Public Safety Incident¹⁵ [emphasis added]. Alcanna also said “Unless a patron is **flagged**, personal information collected by PatronsCan is deleted after 90 days”.

[66] These statements suggest that Alcanna uses the PatronsCan system to “flag” individuals who have been “involved in a prior incident of theft, robbery or violence” so that it can decide to prohibit them from entering its retail liquor stores.

[67] As previously noted, section 69.2(1) of the GLCA applies. This section says:

69.2(1) A licensee may, **before allowing a person to enter licensed premises**, collect the person’s name, age and photograph.

(2) If a licensee has personal knowledge or reasonably believes that a person referred to in subsection (1) has, at any time within the preceding year, **engaged in an activity referred to in section 69(1) or (2)**, the licensee may, in good faith, disclose the person’s name, age and photograph to other licensees for the purpose of allowing them to determine whether they wish to allow the person to enter licensed premises. [emphasis added]

[68] Sections 69(1) and (2) (referred to in section 69.2(2) above) are about “conduct on licensed premises”, and read as follows:

69(1) No liquor licensee or employee or agent of a liquor licensee may permit any activity in the licensed premises that

- (a) is contrary to any municipal bylaw or any Act or regulation of Alberta or Canada,
- (b) is detrimental to the orderly operation of the premises,
- (c) may be injurious to the health or safety of people in the premises, or
- (d) is prohibited under the licence or by the regulations.

(2) No person may do anything in licensed premises that

- (a) is detrimental to the orderly operation of the premises,
- (b) may be injurious to the health or safety of people in the premises, or
- (c) is prohibited under the licence or by the regulations.

[69] In summary, section 69.2(1) of the GLCA authorizes a licensee (Alcanna) to collect name, age, and photograph in order to decide whether to allow a person to enter a licensed premise (liquor store).

[70] Again, the GLCA does not specifically state the purpose for which the information may be collected by the licensee, beyond saying “before allowing a person to enter”; however, section 69.2(2) authorizes a licensee who believes an individual has been involved in past conduct or prohibited activities to disclose the information to another licensee, so that the other licensee can decide whether to allow the individual to enter. Given this, in my view, these two provisions together indicate a licensee is authorized by the GLCA to collect name, age and photograph **and information about past conduct**, in order to decide whether to allow a person to enter premises.

¹⁵ As noted previously, Alcanna defines Public Safety Incident to mean “a prior incident of theft, robbery or violence”.

- [71] In considering Alcanna’s submission, I visited one of its stores and spoke to the employees there as well as corporate employees of Alcanna. I was advised that although the PatronsCan system was implemented, the feature that would allow Alcanna to deny entry to individuals flagged in the system for past conduct was not implemented, although it might be in the future.
- [72] Given this, it does not appear that Alcanna is collecting and using personal information in order to decide whether or not to allow a person to enter based on past conduct.
- [73] Alcanna **says** it is collecting information via PatronsCan to “Identify patrons who have been involved in a prior incident of theft, robbery or violence”; however, Alcanna and its employees confirmed that the feature of the system that would allow Alcanna to identify these patrons is not functional in its stores. As a result, it is not clear to me how scanning driver’s licences at store entrances would allow Alcanna to identify patrons who have been involved in past criminal activity.
- [74] I acknowledge that the GLCA provides statutory authority for a licensed premise to collect name, age and photograph in order to decide whether to grant entry to an individual, in part based on an individual’s past conduct; however, this does not appear to be Alcanna’s purpose for collecting this information, given the way the PatronsCan system has been implemented in its stores.
- [75] Further, I note that the GLCA specifically authorizes a licensed premise to collect name, age and photograph in order to decide whether to allow entry based on past conduct; Alcanna says that it collects name, age, gender, and first three letters of postal code for this purpose. As previously described, the PatronsCan system in fact collects all of the information encoded in a driver’s licence barcode, although it only retains certain data elements. In my view, if the Legislature had intended licensed premises to collect more information than name, age and photograph for the purpose of identifying patrons who have been involved in past activity that contravened the GLCA, it would have specified this when amending the *Gaming and Liquor Act*. It did not.
- [76] I reiterate my previous finding that, in fact, Alcanna is collecting significantly more personal information than even name, age and photograph via the PatronsCan system (i.e. the initial scan collects all of the information encoded on the driver’s licence).

Findings

- The GLCA provides statutory authority for a licensed premise to collect name, age and photograph in order to decide whether to grant entry to an individual, in part based on an individual’s past involvement in criminal activity. This is a reasonable purpose in compliance with sections 11(1) and 16(1) of PIPA. However, it does not appear that Alcanna is collecting and using personal information for this purpose, given the way the PatronsCan system is configured in Alcanna’s stores.
- Further, Alcanna’s collection and use of all the information encoded in a driver’s licence barcode, and retention and use of gender and partial postal code, for the purpose of identifying patrons who have been involved in a prior incident of theft, robbery or violence, is beyond the

extent reasonable to meet its purpose and is a contravention of sections 11(2) and 16(2) of PIPA.

To Identify Underage Patrons

[77] The third purpose for which Alcanna says it collects and uses personal information via the PatronsCan system is to “Identify underage patrons (collection and use of age only)”.

[78] With respect to minors on licensed premises and supplying liquor to a minor, the GLCA says:

74(1) If a person who appears to be a minor requests to purchase or be given liquor from a liquor licensee, the licensee or other person to whom the request is made must, before granting the request, demand that the person who appears to be a minor provide proof of age.

(2) No minor may enter or be in any licensed premises if the licence prohibits minors from entering into or being in the licensed premises.

(3) No liquor licensee may permit a minor to enter or be in any licensed premises if the licence prohibits minors from entering into or being in the licensed premises.

(4) If a person who appears to be a minor enters licensed premises that a minor is not entitled to enter or be in, the liquor licensee must demand that the person who appears to be a minor produce proof of age.

(5) If a person makes a request for identification under subsection (1) or (4) and the person who appears to be a minor fails to produce identification that is satisfactory to the person making the request, the liquor licensee must

(a) not serve liquor to that person, and

(b) refuse the person entry or ask the person to leave if the licence prohibits a minor from entering and being in those licensed premises.

75 No person may give or sell or permit any person to give or sell liquor to a minor in licensed premises.

[79] Section 74(3) of the GLCA prohibits a licensee from permitting a minor to enter or be in any licensed premises (including a liquor store) if the licence prohibits minors. Licensees must “demand that the person who appears to be a minor produce proof of age” (section 74(4)). If a person who appears to be a minor fails to produce satisfactory identification, a licensee must refuse the person entry (section 74(5)(b)).

[80] I find Alcanna’s purpose of collecting and using proof of age in order to verify the age of a patron who appears to be a minor is reasonable, as required by sections 11(1) and 16(1) of PIPA.

[81] I note also that Alcanna’s purpose in this case is not dependent on section 69.2 of the GLCA which limits the personal information a licensee can collect to name, age and photograph; instead, the section of the GLCA that applies requires that an individual “produce proof of age”.

[82] Given this, in my view it is reasonable for Alcanna to require an individual to produce “proof of age”, such as a driver’s licence, and it is reasonable for Alcanna to view identification for the

purpose of verifying age. I acknowledge that viewing “proof of age” such as a driver’s licence represents a short-term collection of all the personal information that appears on the face of the licence.

[83] Despite this, it is my view that it is not reasonable for Alcanna to use the PatronsCan system to collect and use personal information beyond that which would be viewable on the face of a driver’s licence, nor to retain any information after a decision has been made to grant or deny entry to its premises. To the extent the PatronsCan system collects, uses and retains more than this information for this purpose (for example, when the system collects and retains name, age, gender, and partial postal code), Alcanna is in contravention of sections 11(2) and 16(2) of PIPA.

Findings

- Alcanna’s purpose of collecting and using proof of age in order to verify the age of a patron who appears to be a minor is reasonable, as required by sections 11(1) and 16(1) of PIPA.
- It is not reasonable for Alcanna to collect and use personal information for this purpose beyond that which would be viewable on the face of a driver’s licence, nor to retain any information after a decision has been made to grant or deny entry to its premises. To the extent the PatronsCan system collects, uses and retains more than this information for this purpose (for example, when the system collects and retains name, age, gender, and partial postal code), Alcanna is in contravention of sections 11(2) and 16(2) of PIPA.

Issue 2: Does Alcanna obtain consent for the collection, use and disclosure of personal information, or is the collection, use and disclosure otherwise authorized?

[84] PIPA generally requires that organizations obtain consent for the collection, use and disclosure of personal information. Section 7(1) says:

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...
- (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.

[85] The various forms of consent are set out in section 8 of PIPA and include:

- oral or written consent, commonly referred to as ‘express consent’ (section 8(1))
- deemed consent, where it is reasonable that an individual would voluntarily provide the information for a particular purpose (section 8(2)); and
- ‘opt-out’ consent, where the organization must provide easy-to-understand notice to the individual of the particular purposes of the collection, use or disclosure, the individual has a reasonable opportunity to decline or object, and opt-out consent is appropriate for the level of sensitivity of the personal information involved (section 8(3)).

[86] Notwithstanding section 7(1), sections 14, 17 and 20 of PIPA set out circumstances in which an organization may collect, use and disclose personal information **without consent**, including where “authorized or required by ... a statute of Alberta or of Canada” [sections 14(b)(i), 17(b)(i) and 20(b)(i)].

[87] Section 20(f) also authorizes disclosure of personal information “to a public body or a law enforcement agency in Canada to assist in an investigation (i) undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result”.

[88] With respect to its authority to collect personal information, Alcanna says:

- Subsection 14(b) of PIPA allows for the collection [sic] personal information without consent, if the collection is pursuant to a statute, regulation, bylaw or legislative instrument of a professional regulatory organization.
- Section 69.2 of the Gaming, Liquor and Cannabis Act of Alberta (“GLCA”), does allow for the collection of a person’s name, age and photograph before allowing a person to enter a licensed premises.
- The definition of “licensed premises” in subsection 1(p) of the GLCA includes retail liquor stores.

[89] Alcanna also says:

- Subsection 8(3) of PIPA allows for collecting reasonable personal information with consent if the organization: (i) provides an individual with notice that the organization intends to collect the personal information about the individual for those purposes; and (ii) gives the individual a reasonable opportunity to decline or object to having his or her personal information collected for those purposes.
- For the Project, additional information collected is the gender and first three letters of the postal code. This information is only collected if it exists on the ID. Consent is given by patrons for the collection of their personal information by providing them with proper notice of the information being collected and its purpose. Similar to the use of video surveillance, proper notice includes signage that is prominently displayed before the individual scans their own ID. This signage clearly informs patrons about the purposes for the collection, of their personal information. Since these scanners are self-scanning, meaning that the patron must scan their own ID, the patron has a reasonable opportunity to decline having his or her personal information collected for the purposes identified in the signage by choosing to not scan their ID. Signage is placed beside the scanner with instructions on how to scan your own ID...

[90] Alcanna makes a similar argument for the use and disclosure of personal information, saying:

- Subsection 8(3) of PIPA allows for the reasonable use of personal information if the organization: (i) provides an individual with notice that the organization intends to use the personal information about the individual for those purposes; and (ii) gives the individual a reasonable opportunity to decline or object to having his or her personal information used for those purposes. Alcanna notifies patrons about the use of their information in the notice by explaining to them in the notice that ID information is used to decrease violent crime in liquor stores as well as to create a safe environment for Alcanna's staff and clients. A patron has a reasonable opportunity to decline having his personal information used for the purposes identified in the signage by choosing to not scan their ID. Disclosure of personal information to law enforcement or other public bodies to assist in investigations in compliance of legal requirements is reasonable and Alcanna is in compliance with Paragraph 8(3)(c) [sic] and Section 11 of PIPA.

[91] And also:

Alcanna, through Servall, only discloses the personal information it collects through the Project to law enforcement and public bodies in accordance with paragraphs 20(f)(i) and (ii) of PIPA. These provisions allow an organization to disclose personal information if (i) the disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation, and (ii) undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result.

[92] In summary, Alcanna says it relies on sections 14(b)(i), 17(b)(i) and 20(b)(i) for its authority to collect use and disclose name and age without consent (pursuant to section 69.2 of the GLCA), and it obtains 'opt-out' consent (section 8(3) of PIPA) for authority to collect, use and disclose gender and partial postal code. Alcanna also says that it relies on section 20(f) of PIPA for authority to disclose personal information to a public body or law enforcement agency without consent, where the public body or law enforcement agency is conducting an investigation that could lead to, or is likely to result in, a law enforcement proceeding.

[93] As previously discussed, the GLCA is a statute of Alberta that applies to licensees, such as Alcanna, in respect of "licensed premises". Section 69.2(1) of the GLCA authorizes a licensee to

collect name, age and photograph in order to decide whether or not to allow a person to enter licensed premises. I previously said that in my view, this authorizes a licensee to collect, use and disclose name, age and photograph in order to identify a person who may be involved in a criminal activity that needs to be investigated, and to decide whether or not to allow entry based on past conduct.

- [94] Section 69.2(2) also authorizes a licensee to disclose name, age and photograph to other licensed premises so that they can decide whether to allow a person entry based on past conduct, and section 69.2(3) **requires** a licensee to disclose this same information to a police officer on request.
- [95] Section 74 of the GLCA also **requires** a licensee, such as Alcanna, to demand proof of age from any person who appears to be a minor, before granting them entry to licensed premises (such as a liquor store).
- [96] Given the above, I accept that Alcanna has statutory authority pursuant to sections 69.2 and 74 of the GLCA to collect, use and disclose name and age as described above, and the collection, use and disclosure of this information without consent is therefore authorized by sections 14(b)(i), 17(b)(i) and 20(b)(i) of PIPA.
- [97] I am also satisfied that section 20(f) of PIPA authorizes Alcanna to disclose personal information to law enforcement in order to assist in an investigation related to liquor theft.
- [98] Despite the above findings, I do not accept Alcanna's submission that it has obtained opt-out consent as contemplated by section 8(3) of PIPA for the personal information it collects over and above name and age - that is, for the collection and use of all information encoded in the driver's licence barcode, and the retention, use and disclosure of gender and partial postal code thereafter.
- [99] I have already said it is not reasonable for Alcanna to collect, use and disclose this information for its stated purposes; given this, the collection, use and disclosure cannot be authorized by consent under section 8(3) of PIPA. Further, section 20(f) of PIPA cannot authorize Alcanna to disclose personal information to law enforcement where Alcanna is not authorized to collect and use that information in the first instance.

Findings

- Section 69.2 of the GLCA authorizes licensed premises, including Alcanna, to collect, use and disclose name and age in order to identify a person who may be involved in a criminal activity that needs to be investigated, and to decide whether or not to allow entry based on past conduct. This section also authorizes a licensee to disclose name and age to other licensed premises so that they can decide whether to allow a person entry based on past conduct, and requires a licensee to disclose this same information to a police officer on request.
- Section 74 of the GLCA requires a licensee, such as Alcanna, to demand proof of age from any person who appears to be a minor, before granting them entry to licensed premises (such as a liquor store).

- Given that Alcanna has statutory authority pursuant to sections 69.2 and 74 of the GLCA to collect, use and disclose name and age as described above, the collection, use and disclosure of this information without consent is authorized by sections 14(b)(i), 17(b)(i) and 20(b)(i) of PIPA. Section 20(f) of PIPA also authorizes Alcanna to disclose personal information to law enforcement without consent, in order to assist in an investigation related to liquor theft.
- Alcanna does not, however, have statutory authority to collect, use or disclose personal information beyond name and age for these purposes, and cannot rely on consent to authorize the collection, use and disclosure of personal information for unreasonable purposes or to an extent that is not reasonable for meeting its purposes.
- Further, section 20(f) of PIPA cannot authorize Alcanna to disclose personal information to law enforcement where Alcanna is not authorized to collect and use that information in the first instance.

Issue 3: Does Alcanna notify individuals about its collection of personal information, as required by section 13 of PIPA?

[100] Section 13(1) of PIPA says:

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 or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

[101] With respect to notifying individuals of its purpose(s) for collecting personal information, Alcanna says it...

...displays a privacy notice sign/sticker which is placed near the ID scanner so that patrons may see it prior to scanning their own ID. The privacy notice includes a link to the full privacy policy that can be found on PatronsCan's website. Additionally, a link to the complete privacy policy is placed on the top menu of the PatronsCan website. ...

For the first week of Project implementation, Alcanna also employed a security guard that was trained to monitor scanner use and direct people to resources for any privacy related inquiries. This security guard also instructed patrons on how to scan their own IDs and ensured that the patrons read the privacy notice prior to scanning their IDs.

[102] I visited one of Alcanna's stores and observed and photographed the privacy notices in place.

[103] A poster (Appendix B) was displayed prominently near the entrance of the store, such that it could be viewed by individuals before or at the time their personal information is collected. The poster reads:

We Value Your Safety

For your safety and the safety of our staff

We will be scanning IDs prior to entering into this liquor store.

Why are you scanning my ID?

As you may have seen in recent news, liquor stores are experiencing an increase in violent crime within stores. Over the past 2 years, liquor **thefts have increased by over 700%** with the likelihood of **violence increasing** as well. We've seen that 95% of violent incidents are done by less than 1% of the population, and we are committed to creating a safe environment for our staff and clients. Restricting access through ID verification device has been proven to dramatically reduce violence.

What information are you collecting?

PatronsCan limits the collection of information to only what we consider important to verify age and for law enforcement investigations when a crime is committed. Your information collected is limited to your **name, age, gender and first three letters of your postal code.**

How long is the information kept?

Unless you're involved in a crime, your information will be permanently deleted within **90 days**.

In partnership with [EPS logo] [Patronscan logo]

[emphasis in original]

- [104] Although the poster identifies the personal information that will be collected – “name, age, gender” and “first three letters of your postal code”, I have already said previously that the Patronscan system in fact scans all of the information encoded on the driver’s licence barcode, and not just name, age, gender and partial postal code. Further, I previously found that collecting all information from the driver’s licence, and using, disclosing and retaining gender and partial postal code represents a collection, use and disclosure beyond what is reasonable for Alcanna’s purposes.
- [105] The poster also says Alcanna’s purposes for collecting information are “...to verify age and for law enforcement investigations when a crime is committed”. The poster is not clear what information is collected for which purpose. I also note that, if Alcanna was using the Patronscan functionality that would allow the system to flag individuals who are involved in a prior incident theft, robbery or violence, this additional purpose, as identified by Alcanna in its submissions for this investigation, is not mentioned on the poster.
- [106] Section 13(1)(b) of PIPA also requires that an organization notify individuals “of the name or position name or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection”. The poster does not include this information. It may be that the intent of this provision of PIPA was met by employing “a security guard that was trained to monitor scanner use and direct people to resources for any privacy related inquiries”. However, Alcanna said that this was only “For the first week of Project implementation”.
- [107] In addition to the privacy poster, I found another privacy notice placed on the till at the store I visited (Appendix C). This notice is smaller in size than the poster, but provides essentially the same information. A notable difference, however, is that it includes the following information near the bottom:
- Where can I get more information?
Go to patronscan.com/privacy to find out more.
- [108] I visited “patronscan.com/privacy” and found that the webpage informs individuals how they may obtain more information regarding the collection of their personal information, but does not provide the contact information of a person, as required under PIPA.
- [109] I also note that this link is included in a notice at the till, inside the store. Presenting information to individuals after their personal information has already been collected (i.e. in order to enter the store) falls short of the requirement under section 13(1) to notify individuals “Before or at the time of collecting personal information”.
- [110] As with the privacy poster, the notice at the till does not identify the organization that is collecting personal information, although it does display the Patronscan logo. I believe an individual viewing this notice could understand Patronscan to be the organization collecting personal information for its own purposes, and not necessarily Alcanna. At best it is inaccurate; at worst, misleading.

[111] Given the above, I find that the notice posted by Alcanna in stores does not comply with section 13(1) of PIPA in that it does not accurately identify the personal information that is collected, nor the purposes for that collection. It also does not provide the “name or position name or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection”.

Finding

- The notice posted by Alcanna in stores does not comply with section 13(1) of PIPA in that it does not accurately identify the personal information that is collected, nor the purposes for that collection. It also does not provide the “name or position name or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection”.

Recommendation

- I recommend that Alcanna modify the notices posted in its stores to meet requirements under section 13(1) of PIPA.

Issue 4: Has Alcanna made reasonable security arrangements to protect Project personal information, as required by section 34 of PIPA?

[112] Section 34 of PIPA says:

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.

[113] The OIPC has consistently urged entities subject to Alberta’s privacy laws to implement three layers of safeguards: administrative, physical and technical (see OIPC Investigation Reports P2006-IR-005, H2006-IR-002, H2007-IR-002, F2013-IR-01 and F2018-IR-03, for example). I considered the safeguards implemented for the Project with this in mind.

Administrative Safeguards

[114] Administrative safeguards typically include components such as contractual provisions, policies and procedures, and privacy training.

[115] As previously described, Alcanna says that “The nature of the business relationship between Servall and Alcanna, is that Servall is a vendor and Alcanna is their customer. From a data governance perspective, Servall is the data custodian for the data collected by Alcanna using Patronsca. Alcanna understands that in accordance with subsection 5(2) of ...[PIPA] that Alcanna is responsible for Servall’s compliance with the PIPA.”

[116] Alcanna provided me with the contracts between Servall and Alcanna concerning the Project. In addition, Servall provided me with a copy of a sample contract.

[117] I reviewed these documents. They generally constitute an agreement for the “Customer” (Alcanna) to purchase equipment and a software license from Servall. Some notable sections include “Article 5 - DOCUMENTATION AND TRAINING”, which says that “Patronsca will provide the Customer with [user] Documentation” and “the Customer will have unlimited access to Patronsca’s tutorial videos and articles”. Further, “Patronsca will provide the Customer with live user training for the Equipment and Software”.

[118] Article 7 addresses “SECURITY AND PRIVACY”. Section 7.1 describes “Patronsca’s Security Measures”, and outlines Patronsca’s commitment to encryption standards, secure data centres, and ability to remotely and permanently disable access in the event equipment is lost or stolen. This section also says:

- “Personally identifiable data will be permanently removed from Patronsca’s servers according to Applicable law”
- “Aggregated non-personally identifiable data will persist indefinitely on Patronsca’s servers and may be used for business intelligence reports, industry reports and any other promotional applications developed by Patronsca”.

[119] Section 7.2 describes the “Customer’s Privacy Obligations” as follows:

1. The Customer agrees to, and agrees to abide by, Patronsca's privacy policy regarding the collection and use of personal information, as such policy may be amended, modified, supplemented or restated from time to time.
2. The Customer shall have available, or be able to make available, upon request by any patron, police officer, privacy compliance team or liquor control inspector the following documents: Patronsca Privacy Policy and Patronsca Disclosure Request. A current Privacy Policy and Patronsca Disclosure Request form are available at www.patronsca.com/privacy.
3. The Customer shall display a public notice sign provided by Patronsca on or near any Equipment using the Software that scans identification specifying why personal information is being collected, how long it will be retained, and the contact information for Patronsca's privacy officer.
4. Customer agrees to use the Equipment to scan any driver's license or identification card issued by the Department of Motor Vehicles, and to use the PatronScan [sic] service, solely for the following purposes:
 - (A) To verify age or the authenticity of the driver's license or identification card.
 - (B) To comply with a legal requirement to record, retain, or transmit that information.
 - (C) To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation.

[120] Section 7.3 of the contract addresses the "Use of Personal Information". The eight clauses in this section variously address:

- The users who will have access to personally identifiable information (administrators) and those who do not (scan-only users)
- Scan-only users will be able to view incident information if it is stored on Customer Equipment
- Customers shall designate Administrators who will be able to view, create and edit incident information
- The Customer will abide by "Applicable Law regarding the collection and disclosure of personal information"
- The Customer agrees that all users with administrative access shall behave in a responsible and ethical manner when accessing personal information
- Where a patron disputes a ban, Patronsca will refer the matter to the Customer who agrees to review the ban and respond to the patron in a timely manner
- Where a patron "completes, signs and submits a formal ban investigation form to Patronsca", Patronsca will refer the matter to the Customer. The Customer agrees to review the ban and respond to Patronsca within five (5) days. If Patronsca does not hear from the Customer within five (5) days, Patronsca will consider the ban can be removed.
- Patronsca "reserves the right to suspend or restrict access to the Software for any user that creates fraudulent or misrepresentative information about a patron in the Software".

- [121] In addition to reviewing the contract, I asked Alcanna about policies and procedures and training. Alcanna says that because it has implemented the Patronsca n system as a pilot project, it has not yet developed policies and procedures governing its implementation and use. I note that section 6(1) of PIPA requires organizations to develop and follow policies and practices to meet their obligations under that act, and section 6(3) requires organizations to make written information available on request about these policies and practices.
- [122] Alcanna explained that it trained employees working at its stores in relation to the Project system and that its employees are to assist individuals in the following situations:
- if an individual has government-issued identification other than a driver’s licence that the Patronsca n system cannot scan (such as a passport),
 - if there is more than one person seeking to enter a store at once, or
 - if an individual is facing difficulties in gaining entry due to mobility issues, being denied entry by the system (due to being a minor), technical difficulties with the scanner, or otherwise.
- [123] Finally, Servall provided me with detailed information concerning the process it follows in responding to requests for information from law enforcement agencies, which process does not involve Alcanna.
- [124] Overall, my review of the administrative safeguards in place for the Project highlighted a number of gaps.
- [125] First, despite the fact Alcanna states that it understands it is responsible for Servall’s compliance with PIPA with respect to personal information collected, used and disclosed on Alcanna’s behalf, there is nothing in the contract that reflects this relationship or accountability. Instead, the contract binds Alcanna to abide by Patronsca n’s Privacy Policy and disclosure process, and to post Patronsca n’s notice of collection. The purposes for which the Customer (Alcanna) can scan identification are also set out in the contract and include “To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation”, which does not align with the purposes for which Alcanna said it collects personal information during the course of this investigation, nor the purposes described on the privacy notice.
- [126] The “Use of Personal Information” section of the contract does not describe the purposes for which Servall may access and use personal information collected, used and disclosed on Alcanna’s behalf, and does not prohibit Servall from making any other use of the information.¹⁶ As noted above, the contract does say “Aggregated non-personally identifiable data will persist indefinitely on Patronsca n’s servers and may be used for business intelligence reports, industry reports and any other promotional applications developed by Patronsca n”. It is not clear to me how the parties define “non-personally identifiable data”.
- [127] The contract does not include a breach response process (in the event a breach occurs involving personal information for which Alcanna is accountable), nor does it describe a process by which

¹⁶ Although “Article 9 - CONFIDENTIALITY” does say that the “Customer [Alcanna] shall not disclose any business, technical or financial information of Patronsca n”

Alcanna will be able to respond to requests for access to information, which may well require the involvement of Servall and a need to adhere to legislated timelines. It may be that Servall handles these requests on Alcanna's behalf, but this is not clear in the contract.

[128] In addition to these concerns with respect to the contract between Alcanna and Servall, I note that Alcanna said that it does not have any policies and procedures in place respecting collecting, using and disclosing personal information for the Project.

[129] Finally, with respect to Servall's process for responding to requests for information made by law enforcement, I note again that Alcanna said that it is not involved at all in the process, since Servall handles these requests entirely on its own¹⁷. Specifically, Alcanna said:

Servall will behind the scenes, without Alcanna's involvement, manage the law enforcement requests. Law enforcement may request the scan history in the following circumstances:

(i) The public body or law enforcement agency has identified its lawful authority to obtain the information.

(ii) The public body or law enforcement agency has indicated that the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

(iii) The public body or law enforcement agency has provided an investigation number or any other uniquely identifiable number that can be traced back to the purpose of the disclosure request.

[130] I previously found that Alcanna has legal authority under PIPA to disclose certain personal information to law enforcement agencies for specific purposes. However, I did not see anything in the contract between Alcanna and Servall specifically authorizing Servall to disclose personal information to law enforcement agencies on Alcanna's behalf (i.e. Servall's role in this regard is not described in the contract).

[131] Overall, it is my view that Alcanna has not implemented reasonable administrative safeguards to protect personal information collected, used and disclosed as part of the Project.

Physical Safeguards

[132] Alcanna made a number of submissions with respect to the physical security of personal information collected, used and disclosed in connection with the Project.

[133] To begin with, Alcanna confirmed that it "...is not using a service provider outside of Canada to store personal information.... All the personal information is stored in Alberta".

[134] Further, "No personal information is stored on any of Alcanna's servers". In fact:

Alcanna currently does not have access to or the ability to view any of the personal information that is collected by the PatronsCan product. The only information that an Alcanna store employee sees, is

¹⁷ Appendix D shows the PatronsCan form Servall requires law enforcement officers to fill out.

a coloured light that indicates someone is attempting to enter the store may be underage or flagged for a Public Safety Incident.

[135] Instead:

Patronscan's ID scanner collected the personal information from the ID. No personal information is stored on the terminal persistently. Every Patron Entry Record is queued in a non-persistent/encrypted and reserved memory space to be transmitted to Patronscan's secure central server in Calgary. Once transfer is complete the record is permanently deleted from the ID scanner.

[136] Alcanna also says:

Patronscan is a cloud-based solution and all personal data is stored on Servall's central servers. Servall uses Rogers Data Centers. Servall rents a server rack from Rogers and supply their own servers that they configure, control and maintain. The location of all Servall's servers are in Calgary, AB. Physical access to data centre facilities, backup media and other components is controlled using Dual-Two-stage authentication process and proximity cards and access listings. Individuals without proper credentials are restricted from accessing the offices and data center facilities unless accompanied by an authorized representative of Patronscan.

[137] Alcanna also provided a detailed description of physical security measures implemented at the data center to control access.

[138] I confirmed that the Patronscan system hardware in Alcanna's stores is physically out of sight and out of reach of employees and customers. This setup addresses the risk that someone could physically tamper with the computer unit.

[139] With respect to accessing information stored at the data centre, Servall told me that its "Technical staff may need to deal with software issues, database issues, hardware issues, usage issues or any other technical concern that requires the staff member to access the database, or the information contained within it"; however, Servall noted that this "...access is limited to a select few Servall staff, that have gone through privacy training, signed a confidentiality agreement and have their own login credentials that are logged when accessing the server and/or database".

[140] In my view, Alcanna has, through its service provider (Servall), implemented reasonable physical safeguards to protect personal information collected, used and disclosed as part of the Project.

Technical Safeguards

[141] Given the setup of the Patronscan system, Alcanna largely relies on Servall to implement and maintain technical safeguards to protect the Project personal information. Alcanna says:

In addition to the above physical securities, Patronscan also contains the following security practices:

- Under normal operation, Patronscan does not store any data locally on the ID Scanner, all data is sent directly to the cloud storage. Under non-normal operations such as when the Scanner is offline, Patronscan stores data locally on the scanner until network connection is re-established in a non-persistent format. This data is encrypted using AES 256-bit encryption and stored on an encrypted non-persistent and reserved memory space, thus double encrypting the data. Patronscan uses encrypted channels for communication between the ID scanner and central

server which uses TLS 1.2 as the default protocol. Patrons can encrypts the data at rest in the central server. Patrons can uses Microsoft SQL Server 2016 as the database for storing the data on the central server and leverages the encryption capabilities of this industry standard database. All personal data is encrypted at rest.

- Each ID scanning terminal has a remote wipe and disable feature built in. Establishments are required to notify Servall if a terminal is lost or stolen, and then the system is set to be wiped and disabled if the software attempts to access the secure central server.
- No data is held in any exportable format.
- No Patron Entry Record data can be modified or altered. All records are read only.
- All levels of access are password protected, including the ID scanning terminal itself. Every user has a unique account with a unique username/password.
- User accounts are automatically locked if an incorrect password is entered over 10 times in succession.

[142] Project personal information is protected with the use of industry standard data encryption for the length of time the information is stored on the computer, while it transits to the server and for the length of time it remains on that server.

[143] The system includes mechanisms to ensure the data it stores cannot be altered, as well as the ability to remotely wipe a computer if it is reported as missing or stolen.

[144] Servall also explained to me that its systems are programmed to make backups of databases once a day and that newer backups overwrite older backups once the data in a given backup has reached its maximum retention period.

[145] I am satisfied that Alcanna, through its service provider, Servall, has implemented reasonable technical safeguards to protect personal information collected, used and disclosed as part of the Project.

Findings

- Alcanna has not implemented reasonable administrative safeguards to protect personal information collected, used and disclosed as part of the Project, as required by section 34 of PIPA.
- Alcanna has implemented reasonable physical and technical safeguards to protect personal information collected, used and disclosed as part of the Project, as required by section 34 of PIPA.

Recommendations

- I recommend that Alcanna develop and implement policies and procedures for the Project system if it continues using it, or before it implements it in additional stores.

- I recommend that Alcanna revise its contract with Servall to address the gaps highlighted in this report, including accountability for personal information collected, used and disclosed as part of the Project, and to clarify the roles of the parties.

Issue 5: Does Alcanna comply with section 35 of PIPA for any personal information it retains in relation with the Project?

[146] PIPA requires that organizations retain personal information only as long as reasonably required to meet legal or business purposes. Section 35(1) says:

An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.

[147] With respect to the retention of personal information collected as part of the Project, Alcanna said:

Unless a patron is flagged, personal information collected by PatronsCan is deleted after 90 days. This period allows crime victims a reasonable time to report a crime and for law enforcement and other regulatory investigators to review records in incidences. [sic]

[148] When I visited one of Alcanna's stores as part of my investigation, I asked the employees present at that time – the Organization's Vice-President of Loss Prevention, legal counsel and a store employee – how long it typically took to detect instances of theft. I was told that detection was usually "immediate", since an increasing number of thieves operated overtly, sometimes in groups or taking the time to load their vehicles with stolen liquor. The employees also indicated that for any instance of theft that went undetected at the time, it would be difficult to determine the causes of inventory mismatches later, since these could be a result of human error, damaged products or indeed theft.

[149] In May 2020, Alcanna provided additional information, saying that when it reports a liquor theft to a law enforcement agency, it takes seven days on average, and may take up to ten days, for the law enforcement agency to receive Project personal information from the PatronsCan system.

[150] In addition to the above, I reviewed Servall's Privacy Policy, which is accessible on the PatronsCan website¹⁸, and which says the following about retention of data:

What data is stored and for how long?

Unless a patron is flagged, data is retained for a limited period of time before being permanently deleted. This period allows crime victims sufficient time to report a crime and for law enforcement to review patron records to identify the alleged assailant(s). It is common for victims to report crimes several days to weeks later.

Data is permanently deleted after 90 days in most jurisdictions with the exception of:

- 30 days in California (as of January 1st, 2019*)
- 21 days in most Canadian provinces (excluding Alberta and British Columbia)
- 24 hrs. in British Columbia
- 30 days in Australia and New Zealand
- 30 days in the United Kingdom

¹⁸ Content from PatronsCan Privacy Policy under heading "What data is stored and for how long?" Retrieved from <https://patronsCan.com/privacy/> on March 5, 2020.

The only data that is saved beyond the above time frames is specific to patrons that are on the flag list.

- [151] Overall, it appears to me that Alcanna has deferred to Servall with respect to determining the retention period applicable to personal information collected through the PatronsCan system in its stores. I also note that Servall’s retention periods for personal information stored in its systems vary greatly across provinces, from 24 hours in British Columbia, to 21 days in most provinces and 90 days in Alberta, which is the longest.
- [152] As previously noted, Alcanna reported that it does not at this time use the PatronsCan functionality that would allow the system to flag individuals who are involved in an incident. As a result, I assume the only retention period that applies is the 90-day period to allow “...crime victims a reasonable time to report a crime and for law enforcement and other regulatory investigators to review records in incidences”.
- [153] Alcanna’s employees told me that theft detection has to occur immediately, or else Alcanna cannot attribute liquor missing from its product inventory to theft. I understand this to mean that personal information collected via the PatronsCan system is only useful when employees are aware of a theft occurring and the time of the theft. Where store employees are not aware a liquor theft has occurred, personal information collected via PatronsCan will not be of any use, and retaining the information for 90 days is not justified since the usefulness of the information will not increase over time.
- [154] Section 35 of PIPA prohibits organizations from retaining personal information longer than reasonably required for legal or business purposes. In my view, Alcanna only needs to retain personal information collected via the PatronsCan system long enough to allow for disclosure to law enforcement. Alcanna’s employees advised that law enforcement agencies request and receive information about individuals involved in liquor theft within ten days of the theft occurring.
- [155] As a result, I find that retaining personal information collected as part of the Project for 90 days is not reasonable and does not comply with the requirements of section 35 of PIPA.

Finding

- Alcanna’s retention of personal information collected as part of the Project for 90 days is not reasonable and does not comply with section 35 of PIPA.

Recommendation

- I recommend that Alcanna consider how long it needs to retain personal information it collects in the Project to reasonably meet its legal and business purposes and adjust its retention period accordingly.

Summary of Findings

Issue 1

[156] The following seven findings were made on Alcanna collecting and using personal information only for reasonable purposes, and only to the extent reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA:

- Alcanna is a “licensee” and its retail stores are “licensed premises” as defined in the *Gaming, Liquor and Cannabis Act* (GLCA).
- Section 69.2 of the GLCA authorizes licensees to collect name and age before allowing individuals to enter a store and to use and disclose this information in order to “[Identify] patrons who are involved in a criminal activity that needs to be investigated”. This is a reasonable purpose in compliance with sections 11(1), 16(1) and 19(1) of PIPA.
- Alcanna’s initial collection and use of all the personal information elements encoded in a driver’s licence, and its retention, use and disclosure of gender and partial postal code thereafter, is beyond the extent reasonable to meet its purpose of identifying individuals involved in criminal activity and contravenes sections 11(2), 16(2) and 19(2) of PIPA.
- The GLCA provides statutory authority for a licensed premise to collect name, age and photograph in order to decide whether to grant entry to an individual, in part based on an individual’s past involvement in criminal activity. This is a reasonable purpose in compliance with sections 11(1) and 16(1) of PIPA. However, it does not appear that Alcanna is collecting and using personal information for this purpose, given the way the PatronsCan system is configured in Alcanna’s stores.
- Alcanna’s collection and use of all the information encoded in a driver’s licence barcode, and retention and use of gender and partial postal code, for the purpose of identifying patrons who have been involved in a prior incident of theft, robbery or violence, is beyond the extent reasonable to meet its purpose and is a contravention of sections 11(2) and 16(2) of PIPA.
- Alcanna’s purpose of collecting and using proof of age in order to verify the age of a patron who appears to be a minor is reasonable, as required by sections 11(1) and 16(1) of PIPA.
- It is not reasonable for Alcanna to collect and use personal information for this purpose beyond that which would be viewable on the face of a driver’s licence, nor to retain any information after a decision has been made to grant or deny entry to its premises. To the extent the PatronsCan system collects, uses and retains more than this information for this purpose (for example, when the system collects and retains name, age, gender, and partial postal code), Alcanna is in contravention of sections 11(2) and 16(2) of PIPA.

Issue 2

[157] The following five findings were made on Alcanna obtaining consent for the collection, use and disclosure of personal information, or whether the collection, use and disclosure is otherwise authorized:

- Section 69.2 of the GLCA authorizes licensed premises, including Alcanna, to collect, use and disclose name and age in order to identify a person who may be involved in a criminal activity that needs to be investigated, and to decide whether or not to allow entry based on past conduct. This section also authorizes a licensee to disclose name and age to other licensed premises so that they can decide whether to allow a person entry based on past conduct, and **requires** a licensee to disclose this same information to a police officer on request.
- Section 74 of the GLCA requires a licensee, such as Alcanna, to demand proof of age from any person who appears to be a minor, before granting them entry to licensed premises (such as a liquor store).
- Given that Alcanna has statutory authority pursuant to sections 69.2 and 74 of the GLCA to collect, use and disclose name and age as described above, the collection, use and disclosure of this information without consent is authorized by sections 14(b)(i), 17(b)(i) and 20(b)(i) of PIPA. Section 20(f) of PIPA also authorizes Alcanna to disclose personal information to law enforcement without consent, in order to assist in an investigation related to liquor theft.
- Alcanna does not, however, have statutory authority to collect, use or disclose personal information beyond name and age for these purposes, and cannot rely on consent to authorize the collection, use and disclosure of personal information for unreasonable purposes or to an extent that is not reasonable for meeting its purposes.
- Section 20(f) of PIPA cannot authorize Alcanna to disclose personal information to law enforcement where Alcanna is not authorized to collect and use that information in the first instance.

Issue 3

[158] The following finding was made on Alcanna notifying individuals about its collection of personal information, as required by section 13 of PIPA:

- The notice posted by Alcanna in stores does not comply with section 13(1) of PIPA in that it does not accurately identify the personal information that is collected, nor the purposes for that collection. It also does not provide the “name or position name or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection”.

Issue 4

[159] The following two findings were made on Alcanna making reasonable security arrangements to protect Project personal information, as required by section 34 of PIPA:

- Alcanna has not implemented reasonable administrative safeguards to protect personal information collected, used and disclosed as part of the Project, as required by section 34 of PIPA.
- Alcanna has implemented reasonable physical and technical safeguards to protect personal information collected, used and disclosed as part of the Project, as required by section 34 of PIPA.

Issue 5

[160] The following finding was made on Alcanna’s compliance with section 35 of PIPA for any personal information it retains in relation with the Project?

- Alcanna’s retention of personal information collected as part of the Project for 90 days is not reasonable and does not comply with section 35 of PIPA.

Summary of Recommendations

[161] The following five recommendations were made:

- I recommend Alcanna cease collecting personal information beyond those information elements specified in the GLCA.
- I recommend that Alcanna modify the notices posted in its stores to meet requirements under section 13(1) of PIPA.
- I recommend that Alcanna develop and implement policies and procedures for the Project system if it continues using it, or before it implements it in additional stores.
- I recommend that Alcanna revise its contract with Servall to address the gaps highlighted in this report, including accountability for personal information collected, used and disclosed as part of the Project, and to clarify the roles of the parties.
- I recommend that Alcanna consider how long it needs to retain personal information it collects in the Project to reasonably meet its legal and business purposes, and adjust its retention period accordingly.

[162] In June 2021, Alcanna indicated that in relation to recommendation one, “Servall made the decision in February 2021 to collect only the name and age from an ID”. In addition, Alcanna has agreed to recommendations two through five.

[163] I thank Alcanna and Servall for their continued cooperation during this investigation, as well as the AGLC for their assistance.

Chris Stinner
 Manager, Special Projects and Investigations

Appendix A: Scanning Instructions Poster



Appendix B: Privacy Notice - Poster

We Value Your Safety



For your safety and the safety of our staff

We will be scanning IDs prior to entering into this liquor store.

Why are you scanning my ID?

As you may have seen in recent news, liquor stores are experiencing an increase in violent crime within stores. Over the past 2 years, liquor thefts have increased by over 700% with the likelihood of violence increasing as well. We've seen that 95% of violent incidents are done by less than 1% of the population, and we are committed to creating a safe environment for our staff and clients. Restricting access through ID verification device has been proven to dramatically reduce violence.

What information are you collecting?

Patronscan limits the collection of information to only what we consider important to verify age and for law enforcement investigations when a crime is committed. Your information collected is limited to your **name, age, gender** and **first three letters of your postal code**.

How long is the information kept?

Unless you're involved in a crime, your information will be permanently deleted within **90 days**.

In partnership with  

Appendix C: Privacy Notice - Countertop


**Your privacy is as important to us
as your safety.**

Why are you scanning my ID?
As you may have seen in recent news, liquor stores are experiencing an increase in violent crime within stores. Over the past 2 years, **liquor thefts have increased by over 700%** with the likelihood of violence increasing as well. We've seen that 95% of violent incidents are done by less than 1% of the population, and we are committed to creating a safe environment for our staff and clients. Restricting access through ID verification device has been proven to dramatically reduce violence.

What information are you collecting?
Patronscan limits the collection of information to only what we consider important to verify age and for law enforcement investigations when a crime is committed. Your information collected is limited to your **name, age, gender and first three letters of your postal code.**

How long is the information kept?
Unless you're involved in a crime, your information will be permanently deleted within **90 days.**

Where can I get more information?
Go to patronscan.com/privacy to find out more.

 **PatronsScan**

Appendix D: Patronsca’s Law Enforcement Agency Information Request Form



Formal Information Extraction Request

Complete and e-mail to support@patronsca.com or fax 1(877)778-9798

Requesting Officer

Date: Click or tap to enter a date.
First Name: Click or tap here to enter text. **Last Name:** Click or tap here to enter text.
Designation: Click or tap here to enter text. **Police, Liquor or Agency:** Click or tap here to enter text.
City: Click or tap here to enter text. **Email:** Click or tap here to enter text.
Primary Phone: Click or tap here to enter text. **Secondary Phone:** Click or tap here to enter text.
Signature:

**** Please choose Venue History OR Patron History ****

Venue History Request

Venue: Click or tap here to enter text.

Date	Time
From: Click or tap to enter a date.	Click or tap here to enter text.
To: Click or tap to enter a date.	Click or tap here to enter text.

Patron History Request

First Name: Click or tap here to enter text. **Last Name:** Click or tap here to enter text.
Sex: Click or tap here to enter text. **Date of Birth:** Click or tap to enter a date.

Case

Nature of Incident: Click or tap here to enter text. **File Number:** Click or tap here to enter text.
Additional Notes: Click or tap here to enter text.

This information is required to assist in a law enforcement investigation, to enforce or administer and/or to protect the health and safety of Canadians.