Information and Privacy Commissioner,
Ontario, Canada

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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MC17-32

Halton Regional Police Services Board

October 25, 2019

Summary: The Office of the Information and Privacy Commissioner of Ontario received a complaint alleging that the Halton Regional Police Services Board (the police)'s online application process for a police record check, which involves a third party company, collects and uses applicants' personal information contrary to the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

In this Report, I conclude that the police's retention and use of applicants' information is, respectively, in accordance with sections 30(1) and 31 of the *Act*. I also conclude that the police have reasonable measures in place to protect the information, as required by section 3(1) of Regulation 823. However, I find that the police's collection of the information and notice of the collection is not, respectively, in accordance with sections 28(2) and 29(2) of the *Act*. In response to this finding, the police have agreed to implement my recommendations to address this concern.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 56, as amended, sections 2(1), 28(2), 29 (2) and (3), 30(1) and 31; *R.R.O. 1990,* Regulation 823, as amended, sections 3(1) and 5; *Criminal Records Act*, R.S.C. 1985, c. C-47, as amended, sections 6.3(2) and (3); *Criminal Record Regulations*, SOR/2000-303, as amended, section 2(1)(a); and *Police Records Check Reform Act, 2015*, S.O. 2015, c. 30, as amended, section 8(3) and Schedule.

Orders and Investigation Reports Considered: Order 11, P-230, MC09-56, Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe,* [2002] O.J. No. 4300 (C.A.); and Privacy Complaint Reports I96-057M, MC-060024-1, PC-040005-1, I94-001M, MC-050045-1, MC-050047-1, MC10-2, MC13-46, MC13-60, I93-044M, MI10-5 and PR16-40.

Cases Considered: *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27 and *Tadros v. Peel (Police Service)*, 2009 ONCA 442.

BACKGROUND:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a complaint under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) about the Halton Regional Police Services Board (the police)'s online process for a police vulnerable sector check (PVSC).

The Police Vulnerable Sector Check

[2] The PVSC is a type of police record check that individuals can request. It is conducted by police services in Ontario and reveals criminal offence information[1] including convictions, outstanding warrants, charges, judicial orders and sexual offence convictions for which a pardon has been granted where the disclosure complies with the *Criminal Records Act* (*CRA*).[2]

[3] Generally, individuals seeking employment or volunteering in a position of authority or trust relative to vulnerable persons[3] may be required to obtain a PVSC.

[4] The police provide police record checks for Region of Halton residents. On their behalf only, a resident can apply for one either in person or online. The online process is available 24 hours a day and most of it, including identity verification and fee payment, occurs electronically.

The Complaint

[5] In May 2017, the complainant began the process of applying online to the police for a PVSC. While inputting her name, address and other information, she noticed a reference to Forrest Green Solutions (Forrest Green), a third-party company, on the police's website. By this time, the complainant had saved her information to the system.

---

[1] See https://www.haltonpolice.ca/about/courtsrecords/vsc.php.
[2] R.S.C., 1985, c. C-47, as amended.
[3] "Vulnerable Person" means a person who, because of his or her age, a disability or other circumstances, whether temporary or permanent, is in a position of dependency on others or is otherwise at a greater risk than the general population of being harmed by a person in a position of trust or authority towards them. See https://www.haltonpolice.ca/about/courtsrecords/vsc.php.

[6] Based on that reference, the complainant believed that she entered a process in which Forrest Green collected her personal information. As a result, she stopped applying and asked both the police and Forrest Green to delete her information.

[7] Forrest Green explained to the complainant that it collects applicants' personal information to verify their identity on behalf of the police.[4] Forrest Green also confirmed that it removed her information from its systems.

[8] Despite this, she complained to this office about Forrest Green's involvement in the police's online process for a police record check. Specifically, she had concerns about Forrest Green's collection and retention of her information, as well as how the police inform applicants of this collection.

[9] The matter moved to the Investigation Stage of the IPC's complaint process. As part of my investigation, I requested and received written representations, discussed below, from the police.

The Police and Forrest Green's Relationship

[10] Under the Master Services Agreement dated August 7, 2015 between the police and Forrest Green (the MSA), Forrest Green is to maintain "a web based 'Services' website to support [the police] in delivering RCMP compliant solutions to enable online police background checks." The services provided through the Forrest Green Web Portal (the Web Portal) include secure "online credit card payments and online authentication (also known as Electronic Identity Verification…)".

[11] In accordance with the MSA, the police explained that Forrest Green acts as its agent and is authorized to collect and use the information of an individual, who applies online for a police record check, to verify their identity for the check on behalf of the police.

[12] To start the online process, the police advised that its website directs applicants to register an account by providing their name, city of residence, phone number, email address and personalized security questions.[5] At this time, applicants are also required to provide their consent to the Forrest Green End User License Agreement (the EULA)[6], the Forrest Green Consent Statement (FGCS)[7] and the Police Consent to Disclosure Statement (PCDS).[8]

---

[4] Of note, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. Organizations covered by *PIPEDA* must generally obtain an individual's consent when doing so.

[5] https://www.policesolutions.ca/checks/services/halton/register.php.

[6] http://forrestgreensolutions.com/index.php?page=eula.

[7] http://www.policesolutions.ca/checks/services/halton/index.php?page=checkconsent.

[8] http://www.policesolutions.ca/checks/services/halton/index.php?page=checkpolice.

[13] Next, applicants proceed to the Web Portal where they indicate the type of record check that they want. After, as part of the verification process, the police advised that Forrest Green ask applicants for their first and last names, middle and former names, other names that they may use, address, telephone number(s), gender, date of birth, place of birth and current employment information. In addition, an applicant might also provide Forrest Green with their driver's licence number and information about their address and criminal history.

[14] Once applicants provide their information, they must pay a fee (online) before Forrest Green verifies their identity and the police perform the police record check. The police explained that a payment provider independently processes the payment information (that is, debit or credit card numbers) on a separate website inaccessible to the police or Forrest Green.

[15] To verify their identity, the police explained that Forrest Green asks an applicant questions relating to their employment, residence, banking and/or credit history that only the applicant and a licensed consumer credit reporting agency would know the answers to.[9] The police also advised that Forrest Green does not share any of the information that it obtains from the agency with anyone, including the police and that, at no time, does Forrest Green access or see the applicant's credit data.[10]

[16] Once an applicant's identity has been verified, Forrest Green informs the applicant and the police of this, and the police then generate an electronic version of the same form used during an in person police record check to document and convey the results. The police also advised that only its members perform the check and only the applicant receives the results.[11]

ISSUES:

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

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

2. Is the collection of the personal information in accordance with section 28(2) of the *Act*?

---

[9] The online application advises that the applicant's identity is validated using a TransUnion authentication engine.

[10] See section 11 of Forrest Green's End User License Agreement. Credit data includes identifying information, credit history, public records, collections, banking information and inquiries. See https://www.transunion.ca/client-support/credit-reports-scoring.

[11] I note that, where an individual provides written consent, the police can also disclose the results of a police record check to a third party. See section 12(2) of the *Police Record Checks Reform Act, 2015*.

3. Is the notice of the collection in accordance with section 29(2) of the *Act*?

4. Is the use of the personal information in accordance with section 31 of the *Act*?

5. Is the retention of the personal information in accordance with section 30(1) of the *Act*?

6. Are there reasonable measures in place to protect the personal information as required by section 3(1) of Regulation 823?

DISCUSSION:

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

[18] Under section 2(1) of the *Act*, "personal information", in part, means:

> "personal information" means recorded information about an identifiable individual, including,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol, or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> ...
>
> (h) the individual's name if it appears with other personal information relating to the individual or where the

> disclosure of the name would reveal other personal information about the individual;

[19] The list of examples of personal information under section 2(1) is not exhaustive. Therefore, information that does not fall under paragraphs (a) to (h) may still qualify as personal information.[12]

[20] The test to determine whether a given record contains personal information is whether it is reasonable to expect that an individual may be identified if the information is disclosed.[13]

[21] At issue is the information relating to an applicant's name(s), former names, gender, date and place of birth, address, telephone number(s), email address, personalized security questions, current employment, driver's licence number, as well as their employment, banking, residence, credit and criminal history.

[22] In my view, this information would meet the requirements of one or more of the above paragraphs under the definition of "personal information" in section 2(1). The police do not dispute this.

[23] Therefore, I find that the information at issue is "personal information" as defined by section 2(1).

Issue 2: Is the collection of the personal information in accordance with section 28(2) of the *Act*?

[24] Under section 28(2) of the *Act*, the police can collect an applicant's information in only three circumstances, which are:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[25] As noted above, Forrest Green is authorized to collect applicants' information for the police. For this reason, I find that Forrest Green's collection of this information would be a collection by or on behalf of the police.

---

[12] Order 11.

[13] P-230, MC09-56, Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe,* [2002] O.J. No. 4300 (C.A.).

[26] The police submit that its collection of applicants' information is expressly authorized under section 6.3 of the *CRA*.[14]

[27] In Investigation Report I96-057M[15], then Compliance Review Officer, Susan Anthistle considered the phrase "expressly authorized by statute" in section 28(2) and stated:

> ... in our view, the phrase "expressly authorized by statute" in section 28(2) of the Act requires either that specific types of personal information collected be expressly described in the statute, or a general reference to the activity be set out in the statute, together with a specific reference to the personal information to be collected in a regulation under the statute; i.e., in a form or in the text of the regulation.

[28] I accept and adopt this view.

Analysis

[29] Sections 6.3(2) and (3) of the *CRA* state:

> (2) The Commissioner shall make, in the automated criminal conviction records retrieval system maintained by the Royal Canadian Mounted Police, a notation enabling a member of a police force or other authorized body to determine whether there is a record of an individual's conviction for an offence listed in Schedule 2 in respect of which a record suspension has been ordered.
>
> (3) At the request of any person or organization responsible for the well-being of a child or vulnerable person and to whom or to which an application is made for a paid or volunteer position, a member of a police force or other authorized body shall verify whether the applicant is the subject of a notation made in accordance with subsection (2) if:
>
> > (a) the position is one of trust or authority towards that child or vulnerable person; and
> >
> > (b) the applicant has consented in writing to the verification.

[14] Given that the issues concerning the collection of information being expressly authorized by statue can be resolved, in my view, there is no need to consider the other two circumstances in which the collection of personal information is allowed. Moreover, the police did not submit that any of these two circumstances apply.

[15] https://decisia.lexum.com/ipc-cipvp/privacy/en/item/130086/index.do.

[30] Moreover, section 2(1)(a) of the *Criminal Record Regulations* (the *Regulations*)[16] states:

> For the purpose of subsection 6.3(3) of the Act, a consent in writing, by an applicant referred to in that subsection, for a member of a police force or other authorized body to verify whether the applicant is the subject of a notation made in accordance with subsection 6.3(2) of the Act must contain:
>
> > (a) information sufficient to identify the applicant for the purpose of the verification, including the applicant's full name, sex, date of birth, place of birth and address as well as the person's previous addresses, if any, within the last five years;

[31] It is clear that sections 6.3(2) and (3) of the *CRA* set out a general reference to the police record check activity. It is also clear that section 2(1)(a) of the *Regulations* contains a specific reference to listed personal information – that is, "the applicant's full name, sex, date of birth, place of birth, and current address as well as the person's previous addresses, if any, within the last five years" – to be collected for this activity.

[32] However, in addition to that specified information, the police may also collect an applicant's former names, other names that they may use, telephone number(s), email address, driver's licence number and information associated with their personalized security questions, and information about their employment, banking, credit and criminal history.

[33] Based on the term "including" in section 2(1)(a), it appears that this section permits the collection of additional personal information from applicants. Further, given that section 2(1)(a) requires that the written consent to be provided under section 6.3 of the *CRA* contain "information sufficient to identify the applicant for the purpose of the verification", it also appears that section 2(1)(a) permits the collection of as much information that is needed to identify an applicant.

[34] Critically, however, under the *CRA*, the authority to collect applicants' information depends on obtaining their consent. Specifically, section 6.3(3)(b) of the *CRA* requires that "the applicant has consented in writing to the verification", that is, to the police record check.[17]

---

[16] SOR/2003-303, as amended, made pursuant to the *CRA*.

[17] This consent requirement is also found in section 8(3) of the *Police Records Checks Reform Act, 2015*.

[35] Regarding consent, the IPC's "Best Practices for Online Privacy Protection" (the Online Guideline), [18] which provides provincial and municipal institutions with guidance on online privacy protection, is informative in the circumstances of this investigation.

[36] The Online Guideline, generally, advises that "knowledge is when an individual has an awareness and understanding of the facts and implications of something". It also advises that consent "is to give one's permission or to agree to something."

[37] Further, the Online Guideline recommends that institutions:

- provide individuals with clear and adequate information for them to make an informed decision about giving their consent, including the consequences of refusing or withdrawing consent, if any;
- obtain consent prior to collecting individuals' personal information, whenever possible;
- use express consent provisions whenever possible; and
- provide individuals with a simple, clear and secure online mechanism to indicate their consent, refusal or withdrawal of consent, regarding the collection, use and disclosure of their personal information.

[38] Moreover, in Investigation Report I94-001M[19], then Assistant Commissioner, Ann Cavoukian stated:

> For consent to be truly meaningful, that consent must be given on an informed basis and must be given voluntarily. This is the hallmark of consent -- that it be voluntary in nature. If consent is not both informed and voluntary, its value is diminished so greatly that, in our view, it may be rendered meaningless.

[39] I accept and adopt this view.

[40] Accordingly, in my view, the consent required by section 6.3(3)(b) must be informed. While it may not be required in every context, having regard to the sensitive nature of some of the information, it is my view that the form of written consent employed by the police should clearly inform applicants of the types of personal information that may be collected, used and disclosed as part of the online police record check process.

---

[18] https://www.ipc.on.ca/wp-content/uploads/Resources/bpon-e.pdf.
[19] https://decisia.lexum.com/ipc-cipvp/privacy/en/item/129075/index.do?q=I94-001M.

[41] The police submit that applicants provide the consent required by 6.3(3)(b) when they agree to the EULA, the FGCS and the PCDS.

[42] The EULA sets out the terms and conditions for using the Web Portal.

[43] Of note, sections 1.1, 1.2, in part, and 1.3 of the EULA state:

> 1.1 This "EULA" constitutes your agreement with Forrest Green with respect to your use of each of the Forrest Green Web Portal. You must agree to abide by all of the terms and conditions contained in this Subscriber Agreement in order to become or remain an authorized subscriber of any of the Forrest Green Web Portal.
>
> 1.2 To indicate agreement with the terms and conditions of this EULA, you must click the "EULA Consent" checkbox prior to clicking on the "Log Me In". You will not be allowed to register before clicking that button. It is mandatory that each subscriber read the EULA to understand your rights and obligations. If you do not wish to agree to these terms and conditions, do not click the "EULA Consent" and "Log Me In" button (you understand that you will not be subscribed to the applicable Forrest Green Web Portal and will have no right to access such Forrest Green Web Portal unless you agree with the terms of this EULA)...
>
> 1.3 IF YOU HAVE ANY QUESTIONS ABOUT THIS EULA, PLEASE CONTACT YOUR DESIGNATED CONTACT PERSON OR THE FORREST GREEN SOLUTION MAIN TELEPHONE NUMBER OR EMAIL ADDRESS.

[44] Further, section 10 of the EULA deals with privacy and contains hyperlinks to Forrest Green's Privacy Charter, Privacy Statement and Privacy Frequently Asked Questions (FAQs) (collectively, the Forrest Green Privacy Documents).[20]

[45] Together, the Forrest Green Privacy Documents indicate to applicants that their name, address, gender, telephone number, email, age, income, date of birth and financial information may be included in the personal information collected from them.

[46] In addition, section 12 of the EULA states:

> ACCEPTANCE
> 1. You hereby acknowledge that you have read and understand the foregoing EULA and agree to be bound by its terms and conditions.

[20] http://forrestgreensolutions.com/index.php?page=privacycharter & http://forrestgreensolutions.com/index.php?page=privacyfaq.

[47] The FGCS, in part, states:

> I give permission to Forrest Green Solutions Ltd., on behalf of the Police Service, to collect my personal information, including but not limited to name(s), gender, address(es), date of birth, employment history and driver's licence, and to share it with a licenced consumer credit reporting agency (eg. TransUnion) to authenticate my identity when applying online for a police background check. I understand that my personal information will be shared with a consumer credit reporting agency and may update my consumer credit report.

[48] The PCDS, in part, states:

> I hereby authorize the Halton Regional Police Service to inquire into and disclose the results of any police records to me including: outstanding entries, such as charges, judicial orders, peace bonds, probation and prohibition orders; criminal convictions (summary and indictable); absolute and conditional discharges; family court restraining orders; criminal charges resulting in dispositions including, but not limited to, withdrawn, dismissed, and cases of not criminally responsible by reason of mental disorder; police contacts including but not limited to theft, weapons, sex offences, or violent, harmful and threatening behavior, and to conduct a local police contact search with any police service in Canada.

[49] To create and register their account, applicants must agree to the EULA, the FGCS and the PCDS by simply clicking in checkboxes. Collectively, these documents inform them of the following:

- the reasons for the collection, including that the information will be used to verify their identity for a police record check;
- that their consent for the collection and a police check is required; and
- that "consent is obtained via the web page prior to proceeding" and that it can be withdrawn or refused.[21]

[50] Each of these documents also direct applicants to contact the police or Forrest Green should they have any questions.

[51] However, my review of the EULA, the Forrest Green Privacy Documents and the FGCS found that they do not set out all of the information that might be collected from

[21] See the Privacy Frequently Asked Questions and the Privacy Charter.

applicants. Specifically, I did not find any explicit references to the information associated with their personalized security questions, or to place of birth and credit information.

[52] This is of particular concern in relation to credit information because this information is likely to include information collected from third parties, such as credit reporting agencies, rather than from applicants themselves.

[53] As a result, an applicant might not be fully aware of all of their information that might be collected by the police. Accordingly, in my view, an applicant who reads, understands and consents to these documents would not do so on an informed basis, which is expressly required by section 6.3(3)(b).

[54] Accordingly, for the above reasons, I find that section 6.3 of the *CRA* does not expressly authorize the police's collection of applicants' information. Therefore, I find that the police's collection of it is not in accordance with section 28(2).

[55] As such, I will recommend that the police amend the FGCS to explicitly inform applicants of all of the types of information that might be collected from them for a police record check.

[56] Further, with respect to collection practices, the Online Guideline recommends that the police "inform individuals, at or before the time of collection, if the personal information to be collected is required by law and, if so, fully explain the specific requirement."

[57] My review of the police's website and the Web Portal did not find a reference to the *CRA* (or the *Regulations*). As such, I will recommend that the police inform applicants that the collection of their information is specifically required under that legislation.

[58] Moreover, as previously stated, it is also important that the police explicitly inform applicants of the types of information subject to disclosure during the online process. I note that the Schedule under the *Police Record Checks Reform Act, 2015* (*PRCRA*) sets out all of the criminal offence information that might be disclosed following a police check. While this legislation was not in force at the time that the complainant engaged the online process, it is in force now.

[59] My review of the PCDS found that it sets out only some of the offence information in the Schedule under the *PRCRA*. As a result, applicants might not be fully aware of all of their information that might be disclosed.

[60] As such, I will recommend that the police inform applicants of all of the offence information in the Schedule under the *PRCRA* that might be disclosed after a police check has been performed.

Issue 3: Is the notice of the collection in accordance with section 29(2) of the *Act*?

[61] Because the police collect applicants' information, section 29(2) of the *Act* requires that they receive certain notice about the collection, unless certain exceptions in section 29(3) of the *Act* apply.[22]

[62] Section 29(2) states:

> If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

[63] Regarding the notice requirements under section 29(2), the IPC Practices No. 8 "Providing Notice of Collection" (IPC Practices No. 8)[23] is informative in the circumstances of this investigation.

[64] IPC Practices No. 8 states:

> Notice may be provided either orally – in person, over the telephone; or in writing – on an application form, on a posted sign, in a newspaper ad; or in any other manner which informs the individual about the collection.

[65] Moreover, IPC Practices No. 8 recommends that institutions "cite the proper legal authority that permits the collection by referring to the specific act and section that authorizes the collection", or "provide the specific section of an act or by-law which authorizes the activity or program for which the information must be collected."

[66] It also recommends that institutions "fully inform the individual from whom the information is collected about how the information will be used" and ensure that they "will have no difficulty in contacting someone who can provide answers to questions or additional information about the collection."

---

[22] See section 29(3)(a)(b) and (c) for these exceptions.
[23] https://www.ipc.on.ca/wp-content/uploads/Resources/up-num_8.pdf.

[67] The police agree that its webpages[24] concerning the police record check program do not show the legal authority for the collection of applicants' information or the principal purpose(s) for which it is intended to be used. However, the police claim that its webpages contain links to the Royal Canadian Mounted Police (RCMP)'s webpages setting out the legal authority.

[68] My review of the police's webpages determined that they indicate the business address and telephone number for the police's Manager of Information and Records Services, who can address privacy concerns. However, I could not find a link to the RCMP's webpage(s) indicating the legal authority for the collection.[25]

[69] In addition, the police did not submit that any of the exceptions in section 29(3) apply, and there has been nothing in the circumstances of this investigation to suggest that any of them do.

[70] Accordingly, for the above reasons, I find that the police are not providing notice of the collection in accordance with section 29(2).

[71] As such, I will recommend that the police provide notice of the collection to applicants as required by this section.

Issue 4: Is the use of the personal information in accordance with section 31 of the *Act*?

[72] Section 31 states:

> An institution shall not use personal information in its custody or under its control except,
>
> (a) if the person to whom the information relates has identified that information in particular and consented to its use;
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
>
> (c) for a purpose for which the information may be disclosed to the institution under section 32 or under

[24] See www.policesolutions.ca/checks/services/halton/index.php, www.policesolutions.ca/checks/services/halton/index.php?page=crc, www.policesolutions.ca/checks/services/halton/index.php?page=crjmc, and www.policesolutions.ca/checks/services/halton/index.php?page=vsc.
[25] Please note that I could not load: www.rcmp-grc.gc.ca/en/faqs-about-vulnerable-sector-checks & www.rcmp-grc.gc.ca/en/criminal-record-checks cannot be found (i.e. Error 404).

> section 42 of the *Freedom of Information and Protection of Privacy Act*.

[73] The police (through Forrest Green) use an applicant's information to verify their identity to perform a police record check.[26] In my view, such use would be "for the purpose for which it was obtained or compiled".

[74] For this reason, I find that the police's use of an applicant's information complies with section 31(b) of the *Act*.

[75] However, in the course of verifying an applicant's identity, their information collected during the online process is compared against their information held by a credit reporting agency. Where an applicant provides a new or updated home address that differs from the one that the agency has, the police advised that the agency may be informed of this and, as a result, the applicant's credit report might be updated.

[76] In this circumstance, it appears that the police might also use an applicant's information to update their credit report. Such use would not be for the purpose of verifying their identity for a police record check and, therefore, would not be "for the purpose for which it was obtained or compiled". As a result, this type of use would not comply with section 31(b).

[77] The police submit that by agreeing to the EULA, the FGCS and the PCDS, applicants consent to the use of their information to update the address on their credit report. As such, it appears that the police believe that this use complies with section 31(a) of the *Act*.

[78] In Privacy Complaint Report MC-050045-1 and MC-050047-1, Investigator, Mark Ratner found that section 32(b) of the *Act*, which uses similar language to section 31(a) of the *Act* "is implicitly contemplating that applicants provide their informed consent prior to the disclosure of their information to third parties."

[79] I accept and adopt this finding.

[80] Moreover, the Online Guideline recommends that institutions:

> Do not use personal information except in the manner, and for the purpose(s), identified to the individual at the time of collection, unless the individual to whom the personal information relates consents, or by authority of law.

---

[26] I note that the police also use the applicant's information to create their online account. In my view, this use would be part of the identity verification process.

[81] My review of the EULA and the PCDS did not find any reference to the use of applicants' address to update their credit report. But, the FGCS lists "address(es)" as personal information to be collected from applicants and advises that their "personal information will be shared with a consumer credit reporting agency and may update [their] consumer credit report."

[82] As a result, in my view, an applicant who reads and understands the FGCS would know that their address might be used to update their credit report.

[83] Accordingly, I find that an applicant who agrees to the FGCS and proceeds with the online process, identifies their address information and gives their informed consent, as required by section 31(a), to the use of it in updating their credit report.

[84] Therefore, for the above reasons, I find that the police's use of the personal information is in accordance with section 31.

Issue 5: Is the retention of the personal information in accordance with section 30(1) of the *Act*?

[85] Because the police use applicants' information, section 30(1) of the *Act* requires that it is kept "for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information."

[86] To that end, section 5 of Regulation 823 (O Reg 823) states:

> An institution that uses personal information shall retain it for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, except if,
>
> (a) the individual to whom the information relates consents to its earlier disposal; or
>
> (b) the information is credit or debit card payment data.

[87] Together, section 30(1) and section 5 of O Reg 823 establish a default minimum one-year retention period for used personal information[27], subject to the exceptions set out in section 5 of O Reg 823.

[88] The police's Records Retention Schedule policy requires that it keep applicants' information for two years after the completion of the record check process. Further, the

[27] Privacy Complaint Reports MC10-2, MC13-46 and MC13-60.

police advised that Forrest Green keeps applicants' information for more than one year after they pay the fees.

[89] The police advised that where an applicant pays the fees, but they do not complete the online process by having a police check performed, it would keep their information for only 90 days.[28] After this period, the police advised that the information would be destroyed.

[90] Where an applicant starts the online process but does not pay the required fees, the police advised that it would immediately delete and destroy their information.

[91] In Interim Order M-1121, then Assistant Commissioner, Tom Mitchinson considered the matter of "use" and the retention of tape recordings by the Woodstock Police Services Board. In this order, he stated:

> In order to constitute "use" for the purposes [of] section 30 of the Act and section 5 of Regulation 823, the Police must do more than simply collect and store the tapes until the 60-day retention period has expired. It is only when the tapes are "used", including "use" for the purpose of responding to an access request, that the retention schedules must not be strictly applied.[29]

[92] I accept and adopt this approach.

[93] Where the police perform a police record check, it is clear that an applicant's information has been used. In this circumstance, the police and Forrest Green must keep this information for at least one year and they do so.

[94] Where the applicant merely pays the fees but does not proceed to complete the application process, in my view, only their payment information[30] would be used. Such use would be for payment processing related purposes – that is, the payment or refunding of fees.

[95] In my view, this processing activity results in more than a simple collection and storage of this information by the police. In this circumstance, Forrest Green's one-year retention period would comply with section 5 of O Reg 823. Similarly, the police's 90-day retention period would also comply with this section, which permits periods that are

---

[28] A police check might not be performed where an application is incomplete because it is missing identification, the identity verification process was aborted, failed or not completed, or further information is required. See http://www.policesolutions.ca/checks/services/halton/index.php.
[29] https://decisia.lexum.com/ipc-cipvp/orders/en/item/130612/index.do.
[30] For these purposes, payment information means a individual's credit or debit card payment data, such as the cardholder's name and card numbers.

shorter than one year.[31] I also note that, in my view, any other personal information collected in this circumstance, as long as it is not processed or otherwise used, may be (and should be) destroyed at the same time as the payment information.

[96] Where the applicant does not pay the fees or otherwise complete the police record check process, their information would not be used. In my view, this results in a simple collection and storage of the applicant's information and, therefore, would not constitute a "use" for the purposes of section 30(1) of the *Act* and section 5 of O Reg 823. As such, in this circumstance, the police would be permitted to delete and destroy this information.

[97] Accordingly, for the above reasons, I find that the police's retention of the personal information is in accordance with section 30(1).

Issue 6: Are there reasonable measures in place to protect the personal information as required by section 3(1) of Regulation 823?

[98] Section 3(1) of O Reg 823 requires that the police "ensure that reasonable measures to prevent unauthorized access to [applicants' information] are defined, documented and put in place, taking into account the nature of the records to be protected." This requirement "applies throughout the life-cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal."[32]

[99] To that end, the Online Guideline lists steps that institutions can take to keep personal information secure.[33]

[100] In addition, IPC Practices No. 18 "How to Protect Personal Information in the Custody of a Third Party" (IPC Practices No. 18)[34] recommends that agreements between an institution and a third party "should include clauses which cover: collection, retention, use, disclosure, disposal, and security of personal information."

[101] IPC Practices No. 18 also recommends that institutions require:

- third-parties advise their staff or subcontractors of the privacy provisions under the *Act* and their obligation to protect personal information; and

[31] In particular, the police's 90-day retention of the used credit or debit card payment complies with section 5(b) of O Reg 823.
[32] Privacy Complaint Report MI10-5.
[33] See pages 11 to 12.
[34] https://www.ipc.on.ca/wp-content/uploads/2017/01/num-18.pdf.

- all third-party staff or sub-contractors, who will have access to the personal information, sign an undertaking of confidentiality.

[102] In Investigation Report I93-044M, then Assistant Commissioner, Ann Cavoukian considered the term “reasonable measures” in section 3(1) of O Reg 823 as follows:

> The determination of whether reasonable measures had been put into place hinges on the meaning of "reasonable" in section 3(1) of Regulation 823, R.R.O. 1990, as amended. Black's Law Dictionary defines reasonable as:
>
> > Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view ... Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable.
>
> Thus, for reasonable measures to have been put into place would not have required a standard so high as to necessitate that every possible measure be pursued to prevent unauthorized access. In our view, the measures identified above are consistent with Black's definition of "reasonable" -- appearing to be fair and suitable under the circumstances.

[103] Moreover, in Privacy Complaint Report PR16-40, Investigator, Lucy Costa stated the following about section 4(1) of Regulation 460 (which is the provincial access/privacy law equivalent of section 3(1) of O Reg 823):

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

[104] I accept and adopt both of their views.

[105] I reviewed the police's policies concerning security, confidentiality and disclosure of information. I also reviewed certain information that the police provided about the technological, administrative and physical safeguards that it and Forrest Green have in place.

[106] To protect applicants’ information, the police and Forrest Green use, in brief, secure physical hosting, encryption, complex passwords and secure code. They also

regularly review logs and maintenance records, scan for and address security vulnerabilities, and conduct audits.

[107] Based on these policies and the provided information, I am generally satisfied that the police and Forrest Green have defined and documented measures in place to prevent unauthorized access to applicants' information. In my view, these measures are fair and suitable in the circumstances, and align with the steps set out in the Online Guideline.

[108] Further, the MSA and the EULA have provisions prohibiting the unauthorized collection, use, disclosure and retention of personal information. The police also advised that Forrest Green has a confidentiality and non-disclosure agreement that its employees and contractors must sign.

[109] Based on the above reasons, I find that the police have reasonable measures in place to protect personal information as required by section 3(1).

CONCLUSIONS:

1. The information at issue is “personal information” as defined by section 2(1) of the *Act*.

2. The police’s collection of the personal information is not in accordance with section 28(2) of the *Act*.

3. The police’s notice of the collection is not in accordance with section 29(2) of the *Act*.

4. The police’s use of the personal information is in accordance with section 31 of the *Act*.

5. The police’s retention of the personal information is in accordance with section 30(1) of the *Act*.

6. The police have reasonable measures in place to protect the personal information as required by section 3(1) of O Reg 823.

RECOMMENDATIONS:

1. I recommend that, on the FGCS, the police inform applicants of all of the types of personal information that may be collected and used for the purposes of verifying their identity for a police record check and updating their credit-reporting agency address.

2. I recommend that, on the PCDS, the police inform applicants of all of the criminal offence information set out in the Schedule under the *PRCRA* that may be disclosed during the course of a police record check.

3. I recommend that the police, in accordance with IPC Practices No. 8, provide all of the notice requirements under section 29(2) of the *Act* on a single webpage within its website and clearly designate it "Notice of Collection".

The police have reviewed this Report and agreed to implement the above recommendations. Accordingly, within six months of receiving this Report, the police should provide this office with proof of compliance these recommendations.

Original signed by
John Gayle
Investigator

October 25, 2019