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 PR17-23

Ministry of Community and Social Services

June 30, 2020

Summary: The Ministry of Community and Social Services (the ministry) reported a privacy breach under the *Freedom of Information and Protection of Privacy Act* (the *Act*) to the Office of the Information and Privacy Commissioner of Ontario (IPC). The ministry advised that a Family Responsibility Office (FRO)[1] employee inappropriately accessed the case files of multiple FRO clients and disclosed the personal information of some of them to an unauthorized individual. This report finds that the disclosure of information was not in accordance with section 42(1) of the *Act*. It also finds that, at the time of the breach, the ministry did not have reasonable measures in place to prevent unauthorized access to the records. However, in the light of the steps taken by the ministry to address its deficiencies in protecting personal information, no further recommendations are required.

Statutes Considered: *Freedom of Information and Protection of Privacy Act,* R.R.O. 1990, c. F. 31, as amended, sections 2(1) and 42(1); R.R.O. 1990, Regulation 460, as amended, section 4(1).

Investigation Reports Considered: Privacy Complaint Reports MI10-5, I93-044M, PC11-34 and PR16-40.

[1] FRO is a program of the ministry that collects, distributes and enforces court-ordered child and spousal support payments.

BACKGROUND:

[1] On June 13, 2017, the Ministry of Community and Social Services (the ministry) reported a privacy breach under the *Freedom of Information and Protection of Privacy Act* (the *Act*) to the Office of the Information and Privacy Commissioner of Ontario (the IPC or this office).

[2] The ministry advised that a Family Responsibility Office (FRO) employee (the employee) inappropriately accessed the case files of FRO clients.

[3] Later, the ministry provided this office with a Privacy Breach Report dated July 6, 2017 (the Breach Report). According to the Breach Report, on February 16, 2016, the ministry received a complaint from a FRO client (the complainant) alleging that the employee, inappropriately:

- intercepted the complainant's FRO registration package and removed documents from it;
- accessed the complainant's case file in the FRO Case Management System (FCMS); and
- disclosed information about the complainant and other FRO clients' cases to a unauthorized individual.

[4] To investigate the complainant's allegations, the Breach Report provides that the ministry analyzed the employee's:

- FCMS access logs;
- use of information technology (that is, their emails, computer hard drive and web logs); and
- job duties, as they related to the complainant's allegations.

[5] After completing this analysis, the Breach Report provides that the ministry:

- concluded its investigation in November 2016 and, at that time, gave its findings, including confirmation that a breach had occurred, and suggested next steps to FRO;
- in April 2017, gave FRO its final report containing, in brief, the following findings:
    - from November 2013 through February 2016, the employee accessed the cases of ten FRO clients in the FCMS, including their own case, without an authorized business reason;

- between May 2007 and November 2008, the employee sent emails containing the name, addresses and social insurance number (SIN) relating to three FRO clients to an identified individual then working at a debt collection agency;
- in total, 13 individuals were affected by the breach (the affected FRO clients); and
- there was no evidence supporting the complainant's allegation that the employee intercepted her FRO registration package.

[6] In response to the breach, the Breach Report provides that FRO initiated its breach protocol, in brief, by:

- initiating containment of the breach;
- notifying management and its FIPPA[2] Representative of the breach;
- investigating the employee's access to the FCMS;
- in April 2017, discussing the allegations with the employee and terminating their access to FRO client information;[3]
- in June 2017, notifying nine of the affected FRO clients and ministry's Access and Privacy Office of the breach, who in turn, notified the IPC; and
- reviewing its existing privacy breach policies and procedures, including its conflict of interest and internal breach policies, to identify any deficiencies.

The IPC Investigation Stage

[7] After this office received the Breach Report, the matter moved to the Investigation Stage of the IPC's complaint process.

[8] As part of my investigation, I requested and received written representations, discussed below, from the ministry.

[9] The ministry advised that, through its investigation, FRO determined that the employee had personal relationships with two of the affected FRO clients, but did not inform FRO of this or that they had their own FRO case.

---

[2] FIPPA means *Freedom of Information and Protection of Privacy Act.*
[3] The ministry advised that, for approximately five months in 2016, the employee did not have access to government resources through her employment with FRO.

[10] Further, the ministry also advised that FRO could not determine which screen(s) or what information the employee accessed, but confirmed that the FCMS contains information about FRO clients' name(s), address(es), phone number(s), gender, date of birth, SIN, driver's licence number, bank account(s), employment history, income source(s), support arrears, health records, financial statements (for example, income tax statements) and bankruptcy and social assistance status.

[11] The ministry also advised that FRO did not discuss the complainant's allegations with the employee or terminate their access to client information until April 2017, or confirm with the employee that they did not retain, make copies of or further share the affected FRO clients' information.

[12] Because of the employee's actions, the ministry advised that FRO dismissed them in April 2017.

[13] With respect to the disclosure of three of the affected FRO clients' information by the employee, the ministry advised that the identified individual was their friend (or acquaintance), and that this individual was not authorized to receive it.

[14] Further, the ministry advised that FRO made numerous, but unsuccessful, attempts to contact the employee's friend to ensure that they did not retain, make copies of or further share the information.

ISSUES:

[15] 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. Was the disclosure of the personal information in accordance with section 42(1) of the *Act*?

3. Were reasonable measures in place to prevent unauthorized access to the personal information as required by section 4(1) of Regulation 460 under the *Act*?

DISCUSSION:

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

[16] "Personal information" is defined in section 2(1) of the *Act.*

[17] Section 2(1), in part, states:

> "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 where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[18] At issue is the information that the employee disclosed to the individual identified as their friend. This information includes the name, addresses and SIN relating to three of the affected FRO clients.

[19] Also at issue, is the information in the FCMS that the employee may have accessed, which includes the affected FRO clients' information relating to their name, address, SIN, gender, date of birth, driver's licence number, bank account(s), employment history, income source(s), support arrears, health records, financial statements and, bankruptcy and social assistance status.

[20] Based on the above definitions, I am satisfied that all of the information at issue qualifies as "personal information" under the *Act*. The ministry does not dispute this.

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

Issue 2: Was the disclosure of the personal information in accordance with section 42(1) of the *Act*?

[22] There is no dispute that the employee disclosed the information of three of the affected FRO clients by emailing it to their friend. Above, I found that this information is "personal information" as defined by section 2(1).

[23] Section 42(1) of the *Act*, generally, prohibits the disclosure of personal information in the custody or under the control of the ministry unless the circumstances fall within one of the exceptions in the *Act*.

[24] In this matter, the ministry confirmed to this office that none of the exceptions under section 42(1), or otherwise under the *Act*, apply to the disclosure of the personal information at issue.

[25] As such, the ministry also confirmed that the employee's actions amounted to an unauthorized disclosure.

[26] I find that the disclosure of personal information by the employee to the individual was not in accordance with section 42(1) of the *Act.*

Issue 3: Were reasonable measures in place to prevent unauthorized access to the personal information as required by section 4(1) of Regulation 460 under the *Act*?

[27] Section 4(1) of Regulation 460 (O Reg 460) under the *Act* requires that the ministry "ensure that reasonable measures to prevent unauthorized access to the records [in its custody or under its control] are defined, documented and put in place, taking into account the nature of the records to be protected."

[28] 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."[4]

[29] In Investigation Report I93-044M, then Assistant Commissioner Ann Cavoukian considered the term "reasonable measures" in section 3(1) of Regulation 823, which is the municipal access/privacy law equivalent of section 4(1), 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.

[4] Privacy Complaint Report MI10-5.

> 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.

[30] Further, in Privacy Complaint Report PR16-40, Investigator Lucy Costa stated the following about section 4(1):

> 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.

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

[32] In this matter, to determine whether the ministry has satisfied the requirements in section 4(1), the IPC's "Privacy Breaches Guidelines for Public Sector Organizations" (the Privacy Breaches Guidelines) [5], which provides provincial institutions with guidance on how to deal with privacy breaches, as well as past IPC decisions and reports, are informative.

[33] At the time of the breach, to prevent unauthorized access to the affected FRO clients' information, the ministry advised that FRO had (and continue to have) the following measures in place:

- a "Privacy Breaches and Disclosure of Client's Personal Information" policy (the FRO Breach and Disclosure Policy);
- a conflict of interest (COI) policy;
- staff privacy training on the *Act*; and

---

[5] The Privacy Breaches Guideline is available at: https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf. On September 5, 2019, this document replaced and includes the recommendations in the IPC's "Privacy Breach Protocol Guidelines for Government Organizations" guidance document that was applicable at the time the breach in this matter occurred.

- audits of the FCMS.

Policies

[34] The ministry advised that the FRO Breach and Disclosure Policy is provided to staff during their onboarding. This policy deals with "managing and reporting breaches of privacy" and also sets out the steps that FRO staff must take to stop and fix a breach.

[35] Further, the FRO Breach and Disclosure Policy defines "personal information" and explains that a privacy breach occurs "when personal information is collected, retained, accessed, used or disclosed in ways that are not in accordance with the provisions of the [*Act*], for instance, when an individual's personal, case-related information is released or shared with parties external to FRO without legal authority."

[36] The FRO Breach and Disclosure Policy also makes it clear to staff that "[u]nauthorized access or use occurs when a FRO staff member accesses, views or shares personal client information internally where there is no clear business purpose for doing so."

[37] The ministry also explained that FRO has a COI policy "to ensure that a perceived conflict of interest does not arise with respect to the enforcement of any case registered with the [FRO] as a result of an employee's enrolment or the enrolment of a friend or relative of an employee in the enforcement program."

[38] During onboarding, the ministry advised that FRO staff review the COI policy and are required to sign a COI Statement to ensure that any employees who declare a conflict are immediately excluded from accessing any case files that would result in a COI. Further, staff must disclose a COI when they become aware of an actual or potential conflict in their everyday work and where they are aware of a conflict when they begin their employment.[6]

Staff Privacy Training

[39] In Privacy Complaint Report PC11-34 (PC11-34)[7] , then Investigator Jeffrey Cutler made the following findings about what section 4(1) requires with respect to staff training:

> The requirement to put in place reasonable measures to protect information from unauthorized access pursuant to section 4(1) includes a

---

[6] According to the ministry, examples of a COI include where a FRO employee becomes a client of the program or has a personal relationship with a FRO client.
[7] https://decisia.lexum.com/ipc-cipvp/privacy/en/item/133852/index.do

> requirement to ensure that staff are appropriately trained in the management of personal information. This means that staff and management who require access to personal information in order to perform their duties shall receive training to a level commensurate with the sensitivity of the information to which they have access.

[40] Further, with respect to staff accessing computer databases, he stated:

> Giving employees wide and rapid access to computer databases containing sensitive personal information may be necessary and essential;…However, knowing that wide and rapid access to these databases is essential, the ministry is required to take reasonable measures to ensure that its employees do not abuse their access rights and privileges, and to ensure that employees understand their obligations to protect the privacy and security of personal information and understand the consequences of their failure to do so.[8]

[41] I accept and adopt his views, as they are relevant in this matter.

[42] The ministry advised that all FRO staff participate in mandatory privacy training. Specifically, the ministry explained that, during a staff member's onboarding period, FRO's FIPPA Representative and FIPPA counsel inform them of FRO's obligations under the *Act* and how to prevent and remediate privacy breaches.

[43] The ministry also provided this office with copies of the privacy training materials and tools used by FRO. My review of them found that they provide staff with information about:

- what "personal information" means under the *Act*, the types of personal information that clients may provide, and how personal information should be used and disclosed in the performance of their duties in accordance with the *Act*;
- what a privacy breach is, how it may occur, how to prevent it, and what to do when it occurs;
- COIs, the appropriate use of workplace assets and confidentiality; and
- privacy tips on how to disclose personal information in accordance with the *Act* and on how to safeguard personal information.

[44] At the time of the breach, the ministry advised that FRO did not have a formal record of the employee's participation in its privacy training program. However, the

---

[8] Privacy Complaint Report PC11-34.

ministry explained that the employee would have received this training when they were onboarded, as well as several reminders through team meetings, internal newsletters, policy updates and memos from the ministry's Assistant Deputy Minister (ADM), regarding the appropriate use and protection of FRO clients' information.

[45] The ministry advised that FRO now tracks staff participation in its privacy training program in order to ensure that all of them receive this training.

Audits

[46] As indicated above, FRO audits the FCMS. The ministry explained that, although a FCMS audit log provides limited information about the specific types of information viewed by users, it does provide the:

- user name of the employee who accessed a case;
- date and time of access;
- case owner's name and user log ID; and
- case number of the accessed FRO case.

[47] The ministry advised that audits of the FCMS could be random on specific cases and/or users, or, more broadly, through FRO's quality assurance process, which includes call monitoring and reviewing case files and client interactions. The ministry also advised that ongoing and targeted audits are conducted on the FCMS as part of performance management and when privacy issues have been identified.

The Ministry's Response to the Breach

[48] In this matter, the employee accessed the personal information of ten of the affected FRO clients' without authorization and disclosed the personal information of three of the affected FRO clients in contravention of section 42(1) of the *Act*. Therefore, as reported by the ministry, it is clear that privacy breaches occurred.

[49] The duty under section 4(1) of the Regulation is similar to the duty under Ontario's health privacy law to take reasonable steps to protect personal health information from unauthorized use or disclosure. The IPC has stated, with respect to this latter, that the duty to take reasonable steps includes a duty to respond adequately to a complaint of a privacy breach. The IPC's Privacy Breaches Guidelines provide guidance about the type of steps institutions should take in responding to privacy breaches or complaints of privacy breaches. Generally, these are: ensuring that the breach is contained; notifying affected individuals; investigating the cause of the breach; and taking remedial measures to prevent a re-occurrence.

a. Containment

[50] To contain a breach, the Privacy Breaches Guidelines recommends that institutions identify the nature and scope of the breach and take the following action:

- determine what personal information is involved;
- ensure that no personal information has been retained by an unauthorized recipient and getting their contact information in case follow-up is required;
- ensure that the breach does not allow unauthorized access to any other personal information by taking appropriate action;
- in a case of unauthorized access by staff, consider suspending their access rights; and
- retrieve hard copies of any personal information that has been disclosed.

[51] The FRO's own Breach and Disclosure Policy recommends that containment of a privacy breach should be a priority over other tasks.

[52] In this matter, the complainant notified the ministry of the potential breach in February 2016. Although the ministry undertook an investigation into the complaint, and despite the seriousness of the allegations, FRO did not interview the employee or terminate their access to FRO client information until April 2017.

[53] Based on the lengthy delay between the ministry becoming aware of the breach and taking steps to contain it, it appears that the ministry did not prioritize containment.

[54] This also appears to be the case as the ministry did not take steps to ensure that the employee did not retain, make copies of or further share the affected FRO client's personal information.

[55] In response to both of these concerns, the ministry advised that, going forward, it will take stringent steps to prioritize the containment of a breach, including revoking an employee's access to the applicable database (for example, the FCMS) to prevent further unauthorized access, as well as asking them to return any inappropriately accessed personal information and ensuring that it is not copied or shared.

b. Notification

[56] In PC11-34, the Investigator stated "that the obligation set out in section 4(1) of Regulation 460 to put in place reasonable measures to protect personal information from unauthorized disclosure, includes an obligation, barring exceptional circumstances,…to provide the affected individual with the details of the steps taken in response to the breach, including the results of the internal investigation and any

disciplinary action taken against the employee in question."[9]

[57] I accept and adopt this finding.

[58] In this matter, the ministry advised that FRO was able to confirm the address of nine of the affected FRO clients and mailed them a notification letter dated June 30, 2017.

[59] The ministry explained that four of the affected FRO clients were not notified because one of them is the employee and FRO:

- was unable to identify two of them from their disclosed information; and
- for one of them, it could cause harm, based on certain health and safety concerns.

[60] The notification letter sent to the affected FRO clients did not contain details about the personal information at issue or the steps taken to address the breach.

[61] I also note that although the affected FRO clients' personal information involves financial and government information, FRO did not suggest any precautionary measures that the affected clients could take to protect their information.

[62] I raised these concerns with the ministry and was advised that FRO has reviewed its breach notification letter and updated it to include details about the information at issue and the steps taken to contain and remediate the breach.

[63] Further, the ministry confirmed that, where a breach involves financial and/or government information, it is committed to reviewing the circumstances of the breach to determine whether it is appropriate to inform the affected individual of the precautionary measures that they can take.

c. Investigation

[64] As stated above, the duty to take reasonable measures to protect personal information includes undertaking proper investigations into allegations of a privacy breach. In this matter, the ministry and FRO investigated and determined that a breach occurred. Moreover, the ministry advised that FRO's Breach/Case Manager and FIPPA Representative, as well as the ministry's Access and Privacy Office were notified of the breach.

[65] The ministry's investigation appears to have been comprehensive although, as I

---

[9] Privacy Complaint Report PC11-34.

stated above, I am concerned that it did not consider whether it should suspend the employee's access rights immediately on receiving the details of the complaint.

d. Remediation

[66] The ministry advised that, on March 22, 2018, the ministry's ADM sent FRO staff a memo regarding the "Proper Use of databases, Conflict of Interest and Annual Staff Privacy Training".

[67] This memo reminds FRO staff of their responsibility to comply with the *Act*, safeguard client information, keep up-to-date with FRO's privacy policies and of the ADM's zero tolerance policy for the unauthorized access or disclosure of personal information.

[68] Going forward, the ministry advised that FRO is working to implement a consistent practice of staff privacy discussions, COI declaration renewals on an annual basis and Standards of Ethics and Conduct (eLearning) training[10]. In addition, the ministry explained that, in July 2019, FRO launched a program-specific privacy e-learning course that staff are required to complete on an annual basis.

[69] As indicated above, FRO now tracks privacy training. The ministry explained that it does so by tracking the completion of mandatory e-learning sessions as well as the attendance for new employee training to ensure that all staff complete the mandatory onboarding training sessions.

[70] Moreover, the ministry advised that FRO's FIPPA Representative has developed various tools and outreach initiatives to assist front-line staff with day-to-day questions and concerns they may have regarding privacy issues, they include:

- creating a dedicated privacy page on FRO's intranet that offers staff various online privacy tools and reference materials; and
- including privacy tips and reminders in FRO's newsletter that address everyday privacy questions and concerns at FRO.

[71] In the wake of this incident, the ministry advised that FRO identified a gap in its policies relating to breach containment, as the employee had continued unauthorized access to the FCMS.

[72] Specifically, the ministry explained that this gap was due to FRO, incorrectly, identifying the breach as an internal disciplinary issue to be handled through human

[10] The ministry advised that this training covers many aspects of privacy, confidentiality and conflict of interest issues in the Ontario Public Service work environment.

resources. The ministry further explained that FRO realized that the privacy policy and procedures that were in place at the time of the breach did not address circumstances involving a staff member who inappropriately accessed a client's personal information.

[73] As a result, the ministry advised that FRO has amended its privacy breach and audit policies to:

- clearly outline the steps to be taken from the identification of the breach through to determining disciplinary actions, including reporting it to the IPC;
- provide a more comprehensive and streamlined approach to addressing the inappropriate access and disclosure of personal information;
- identify FRO's roles and responsibilities when dealing with unauthorized access by an employee; and
- provide guidelines for FRO staff access and use of the FCMS and other shared databases, specifically, outlining that databases are only to be used for their specific job duties.

[74] In addition, FRO made amendments to the Breach and Disclosure Policy to make it clear that staff should not "access or attempt to access any information relating to any case registered with FRO, or contained in any database accessible by employees of FRO, unless such access is required for the employee to carry out his or her duties within FRO."

[75] The ministry advised that FRO has also implemented a Privacy Warning/Agreement on the FCMS. The ministry explained that this warning has terms and conditions that identify the key responsibilities of staff under the *Public Service of Ontario Act* as well as the COI rules for public servants.

[76] At the time of the breach, FRO had in place a number of measures collectively aimed at fulfilling its obligations under the *Act* with respect to the security and confidentiality of its clients' personal information. These included privacy training, auditing, and its Breach and Disclosure Policy.

[77] Despite the above, it is clear that the ministry's practices and policies had some deficiencies. As the ministry recognized, its privacy policy and procedures in place at the time of the breach did not address circumstances involving a staff member who inappropriately accessed a client's personal information. Among other things, this meant that despite recognizing that containment is an important step in responding to a breach or suspected breach, the ministry did not take steps to terminate the employee's access to the FCMS when it became aware of the breach in February 2016. In my view, this gave the employee the opportunity to continue to abuse their access rights and privileges to the FCMS.

[78] Further, in responding to the breach, no steps were taken to ensure that the employee did not retain, make copies of or further share the affected FRO's client's personal information. Moreover, the notices sent to these clients did not inform them of the types of personal information at issue or provide details regarding the steps taken by the ministry in response to the breach.

[79] As a result, for the aforementioned reasons, it is my view that the ministry's policies and procedures fell short in some areas. Most significantly, the ministry's failure to have policies that addressed potential unauthorized accesses by staff to client information, as well as, during the investigation, the ministry's failure to consider termination of access rights. Therefore, I find that the ministry did not have reasonable measures in place to prevent unauthorized access to the personal information as required by section 4(1) of O Reg 460 under the *Act.*

[80] During this investigation, the ministry and FRO took the steps discussed above to address the concerns raised in this report. As such, I am satisfied that no further recommendations are required.

CONCLUSIONS:

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

2. The ministry's disclosure of the personal information was not in accordance with section 42(1) of the *Act*.

3. The ministry did not have reasonable measures in place to prevent unauthorized access to the personal information in accordance with section 4(1) of O Reg 460 under the *Act*.

4. In light of the steps taken by the ministry to address its deficiencies in responding to the breach, no further recommendations are required.

Original Signed by: June 30, 2020

John Gayle
Investigator