OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2018-006

November 9, 2018

Department of Transportation and Works

Summary: The Department of Transportation and Works relocated a number of paper records to its Grand Falls-Windsor Depot. The records, containing sensitive personal information, were stored in an unsecured area accessible to all employees and members of the public. An employee working at the Grand Falls-Windsor Depot notified the Department that some boxes were unsealed and that personal information, including social insurance numbers, could be viewed by anyone with access to the unsecure area. Despite this notification, nineteen days expired prior to transferring the records to a secure storage area. After an employee informed the Commissioner of the breach, the Department subsequently declined to follow the Commissioner's recommendation that it notify impacted individuals of the privacy breach. While the Department agreed, after commencement of this investigation, to notify impacted individuals, its response generally constituted a disregard of its responsibilities pursuant to the *Access to Information and Protection of Privacy Act, 2015*.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c A-1.2, section 64.

Authorities Relied On: Protection of Privacy Policy and Procedures Manual

File #0035-092-18-009

I BACKGROUND

[1] The chain of events leading to the breach started with the Department's decision, in April of 2018, to re-open the Bishop's Falls Depot. In the course of inspecting the building to ensure its readiness, a Department employee discovered fifty boxes of records (including personnel files) stored in an unsecure manner. The Department advises that while the Bishop's Falls depot was closed for several years, it was locked and no evidence of unauthorized access was found.

[2] The Department decided to transport these records to the nearby, and larger, Grand Falls-Windsor Depot (GF-W). The transfer took place on April 19, 2018. Staff at the GF-W Depot were not notified that the boxes contained personal information. The plain boxes had no labels or markings. Some boxes travelled in the back of a pick-up truck. Staff placed the boxes on pallets in the GF-W depot. A number of boxes were in *rough condition*, with the records inside visible and accessible to anyone with access to GF-W's main stockroom. While shrink-wrapped four days later, due to their rough condition, the contents of some boxes remained visible and easily accessible. The records remained unsecured in the main stockroom area, (a high traffic zone for staff as well as couriers dropping off parts/picking up parts) until May 4, 2018, when they were moved to a less accessible but still unsecure area of the GF-W depot. The boxes were moved to a secure area on May 9, 2018 - five days after the Commissioner directly notified the Department's Executive of the breach.

[3] On April 23, 2018 a Departmental employee advised a manager that boxes containing personal information were open and accessible in an unsecure area. Specific examples included a resignation letter, documents containing social insurance numbers, other employment-related information and medical information in the form of doctors' notes. Other than applying shrink-wrap, it appears that internal discussions between the manager and other Departmental officials led to no action to fulfill the Department's legal obligation to employ reasonable safeguards to protect this sensitive personal information.

[4] By May 4, 2018, the Departmental employee notified this Office, due to inaction regarding the continuing risks posed to impacted individuals, including potential misuses of

the personal information to facilitate identify theft and other malfeasance. The Commissioner wrote to the Department's Executive on May 4, 2018, advising of the notification by the employee and, in the event that the employee's report was accurate, requested that the Department:

- ensure that all personal information is secured immediately by personnel with the authority to view/access it;
- determine what personal information is visible, the potential for harm and the need to notify individuals; and,
- provide this Office with a breach notice which is required for all breaches.

[5] The Department submitted the mandatory notice of the privacy breach to this Office on May 11, 2018. On May 14, 2018 the Commissioner wrote the Department and recommended, pursuant to section 64(5), that the Department identify and notify impacted individuals of the privacy breach.

[6] On June 13, 2018 the Department was asked to report on its progress in identifying and notifying impacted individuals. On June 26, 2018 the Department replied stating that it would not notify any individuals as only a small number of the boxes contained personal information, and the personal information in those boxes lay under blank forms and envelopes, thus not easily accessible.

[7] The representation that the personal information was not easily accessible is contradicted by the photographs provided to this Office of the pallets of boxes, the representations of the employee who notified our Office, and the Department's own notice, stating in part that:

> *The* [*name*] *reviewed an additional file placed on top of the box and noticed SIN number only, again, not viewing any personal information. The* [name] *understood the nature and sensitivity of those records and placed them back into the box immediately. At that point, the boxes were shrink wrapped, but still left in an open, unsecure area.*

[8] We notified the Department of the intent to commence an own motion investigation on June 27, 2018. While not directly encompassed by this Report, I note it appears that the

Department also transferred boxes containing similar personal information from the Department's Lumsden Depot to an unsecure area of the GF-W Depot.

II PUBLIC BODY'S POSITION

[9] While it declined to follow this Office's initial recommendation to identify and notify affected individuals, during our investigation the Department agreed to attempt to notify affected individuals.

[10] The Department noted that many depots and other facilities are heavily reliant on paper records and it is taking steps to make an inventory of such records and to develop retention schedules for their destruction, where appropriate.

III DECISION

[11] This investigation concerns several elements of a public body's duty to employ reasonable safeguards to protect personal information and its duties when reasonable grounds exist to believe there has been a breach involving the unauthorized collection, use or disclosure of personal information,

Protection of Personal Information/Storage of Records

[12] Public bodies are legally obliged to protect personal information from unauthorized use or disclosure. They are also legally obliged to ensure that records containing personal information are transferred and stored in a secure manner. Section 64 of the *Act* states:

> *64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*

> (c) *records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.* [emphasis added]

[13] In terms of the failure to comply with the duties imposed by section 64, the examples include:

- Leaving boxes of records containing personal information in an unsecure area of an unoccupied facility;
- The intermingling, without any labelling, of boxes of records containing personal information with other boxes of records;
- Failing to ensure sufficient quality/condition of boxes used to store and transfer personal information;
- Transferring boxes containing personal information in the back of a pick-up truck;
- Failing to inform staff at the GF-Depot that records containing personal information were stored in the boxes; and,
- Failing to act promptly to secure the records on April 23, 2018.

[14] Departmental representatives acknowledged the Department has an issue with managing and protecting a large volume of paper records. Department employees are reluctant to destroy historical records recording leave balances and other details of employment. Further, many of the Department's facilities are in remote locations without internet access, making it difficult to maintain electronic records. Department employees working out of these facilities may lack adequate training with information technology and electronic record keeping.

[15] Despite this, the Department indicated that earlier this year, and prior to this breach occurring, it started an initiative to take an inventory of its paper records and take steps to destroy superfluous or obsolete records where appropriate. This has taken the form of instructions, training, and the acquisition of shredders. The Department is also undertaking a review of its record retention policies to ensure they address all forms of records and provide for their proper storage and secure disposal.

Mandatory Breach Reporting

[16] The head of a public body must notify this Office when they reasonably believe a breach has occurred:

> *64(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.*

[17] In this case, the Department was obliged to notify this Office when the employee advised on April 23, 2018 that he could clearly see personal information in the torn boxes that were stored in an unsecure area of the GF-W Depot. Notice did not arrive until 7 days after this Office had been in contact with the Department's senior executive.

[18] After reviewing the notification and considering the details as reported by the employee, this Office, on May 14, 2018 recommended that the Department identify and notify impacted individuals. Having received no response to this recommendation this Office pursued the matter again with the Department on June 13, 2018. On June 26, 2018 the Department advised that it would not follow the recommendation, relying in part on representations that appeared inconsistent with other information previously received by this Office.

[19] The Department failed to recognize the significance of sensitive personal information being visible and accessible in an unsecured area to which staff and members of the public had access. Besides our health information, we guard little of our personal information more closely than our social insurance numbers. Few Canadians fail to realize that unauthorized disclosure or copying of a social insurance number is a key ingredient of identity theft and other forms of fraud. Section 64(7) allows a public body to forgo individual notification where it reasonably believes that there is not a significant risk of public harm. Significant harm is defined in section 64(8) as:

> *64(8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.* [emphasis added]

[20] The Act provides that this Office can recommend notification of individuals despite a public body deciding that notice is not required:

> *64(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not required, the commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.*

[21] The Department failed to follow the recommendation to notify individuals at the first reasonable opportunity and had to be pursued for its response.

IV CONCLUSIONS

[22] The Department's response to learning of this breach was markedly deficient. Besides ignoring its legal obligations, when, as here, an employee recognizes the need for remedial action because of a privacy breach, what is the Department communicating to its employees by failing to respond appropriately? There is significant doubt that had the employee not contacted this Office, the Department would never have notified us of this breach. Employees should be recognized and commended for recognizing the need to protect personal information. Reports of breaches by staff should be promptly actioned and commended.

[23] In the case of government departments, the Minister is the head of the public body for the purposes of the *Act*. Ministers appropriately delegate responsibility to Departmental officials to ensure compliance with the law. Ministers must have confidence that responses to breaches involving personal information comply, at a minimum, with the *Act's* legal obligations. In these circumstances, Departmental officials fell far short of complying with the *Act's* requirements. The lone exception to the general dereliction being the employee who raised the issue with the Department on April 23, 2018.

V RECOMMENDATIONS

[24] Under the authority of section 76(2), I recommend that the Department of Transportation and Works:

1. ensure that its policies and procedures regarding the protection of personal information are compliant with its obligations under the *ATIPPA, 2015*;
2. ensure it has proper breach protocols in place and that they are followed; and
3. designate appropriate personnel to process the records according to the Department's retention schedule and securely dispose of any records containing personal information that are eligible for destruction according to that retention schedule.

[25] As set out in section 78(1)(b) of the *ATIPPA, 2015*, the head of the Transportation and Works must give written notice of his or her decision with respect to these recommendations to the Commissioner within 10 business days of receiving this Report.

[26] Dated at St. John's, in the Province of Newfoundland and Labrador, this 9th day of November 2018.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador