ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2017-03

May 3, 2017

ACOSTA CANADA CORPORATION

Case File Number 000235

Office URL: www.oipc.ab.ca

Summary: A laptop was stolen from an employee of the Organization. The personal information of the Complainant and other individuals was stored in the laptop. The Adjudicator found at the time of the theft, the Organization had not been in compliance with sections 34 and 35 of the *Personal Information Protection Act.* The Organization revised its policies regarding security measures to prevent risk of loss of personal information and retention of personal information. The Adjudicator found these revised policies were in compliance with the Act. She ordered the Organization to destroy the Complainant's personal information.

Statutes Cited: AB: *Personal Information Protection Act*, S.A. 2003, c. P-6.5 ss 2, 34, 35, 52

Authorities Cited: AB: Orders: P2006-008, P2006-011, P2009-013/P2009-014

I. BACKGROUND

[para 1] A laptop containing the personal employment information of the Organization's current and former employees, including the Complainant's information, was stolen from an employee of the Organization. The information on the laptop included the Complainant's name, birthdate, email address, and social insurance number. The Organization notified the Complainant of the theft of the laptop containing her information.

[para 2] The Complainant made a complaint to the Commissioner that the Organization had failed to protect her personal information against the risk of unauthorized disclosure within the terms of section 34 of the *Personal Information Protection Act* (the Act or PIPA). She also complained that the Organization had contravened section 35 of PIPA, as it had retained her personal information for longer than was reasonably required.

II. RECORDS AT ISSUE

[para 3] As this matter deals with a complaint, there are no records at issue.

III. ISSUES

1. Did the Organization comply with section 34 of the Act (reasonable security arrangements)?

2. Did the Organization comply with section 35 of the Act (retention and destruction of information)?

IV. DISCUSSION OF ISSUES

1. Did the Organization comply with section 34 of the Act (reasonable security arrangements)?

[para 4] Section 34 of the Act reads as follows:

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

[para 5] This inquiry involves the Organization's loss of the Complainant's personal information. The question to be answered is whether the Organization made reasonable security arrangements to protect against the risk of unauthorized disclosure (the loss of the laptop initially) as well as to protect against the risk of unauthorized disclosure and use after the loss of the laptop (e.g., to prevent third parties from using the information).

[para 6] In deciding whether an organization made reasonable security arrangements under section 34, section 2 of PIPA must be considered. It reads as follows:

> *2 Where in this Act anything or any matter*
>
> *(a) is described, characterized or referred to as reasonable or unreasonable, or*

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

The above provision means that I must review the actions taken by the Organization from an objective standpoint, bearing in mind the nature of the Complainant's personal information that was disclosed, the risk of harm to her, and all of the relevant circumstances.

[para 7] The Complainant's information on the laptop included the following:

- Name
- Address
- Date of Birth
- Social insurance number
- Employee identification number
- Email address
- New hire documents
- Employee benefits forms
- Merit increase forms
- Beneficiary form
- Resignation forms
- Pension Plan application form
- Attendance tracking documents
- Performance Management reviews
- Retirement plan information
- Internal promotion memos

[para 8] An organization has the burden of proving that it made reasonable security arrangements to protect personal information in its custody or under its control, as it is in the best position to provide evidence of the steps that it has taken (Orders P2009-013 and P2009-014 at para. 109). To be in compliance with section 34, an organization is required to guard against reasonably foreseeable risks; it must implement deliberate, prudent and functional measures that demonstrate that it considered and mitigated such risks. The nature of the safeguards and measures required to be undertaken will vary according to the sensitivity of the personal information (Order P2006-008 at para. 99).

[para 9] The laptop containing the Complainant's personal information was stolen from a personal automobile of an associate of the Organization. The laptop and other personal items were taken. The theft was discovered on November 11, 2014 and promptly reported to law enforcement and the Organization. The laptop has never been recovered. The

Organization submits to me it is not aware of any misuse of the information stored on the laptop.

[para 10] In this case, the Organization's submissions regarding the measures taken to guard against foreseeable risks at the time of the loss are as follows:

> At the time of the subject incident, Acosta had implemented various policies and procedures, including asset management and access controls, designed to help prevent the unauthorized disclosure of PII. The Company confirmed that the laptop was password protected with a complex password at the time of the theft, but it was not encrypted.

[para 11] The Organization states it has always and continues to take the privacy and security of the sensitive information in its care as a top priority. However, I have no details regarding the "various policies and procedures" that were implemented at the time of the loss. I find the Organization has not met its burden in convincing me at the time of the loss, it had made reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[para 12] I note the Organization provided the Complainant with an avenue to mitigate the loss. Notice of the theft was provided to the Complainant on December 19, 2014. The Organization, in that notice of theft, provided the Complainant with access to a complimentary year of identity protection and fraud restoration services, including non-expiring identity repair services for use at any time in the future. At the same time the Organization provided notice of the theft to the Information and Privacy Commissioner of Alberta. This addresses the second part of the issue noted in para. 5 above (whether the Organization took reasonable steps to protect against the risk of unauthorized disclosure and use after the theft).

[para 13] In submissions to this inquiry, the Organization tells me the following regarding the security measures *now* in place:

> Although no one can ensure that information breaches do not happen, Acosta has taken and continues to take steps to better protect sensitive data. Specifically focusing on the issues related to this inquiry, Acosta has:
>
> • Increased the number of staff dedicated to information security, including the hiring of a new Chief Information Security Officer;
> • Conducted a security awareness training course for employees with access to personal information (to be repeated annually);
> • Encrypted certain end user devices that contain or have access to personal information, including Human Resources personnel;
> • Increased security for certain databases that contain personal information.

[para 14] These measures reflect this Office's guidelines for safety measures to be implemented to protect personal information. I am satisfied the Organization has *now* made reasonable security arrangements to protect personal information that is in its custody or control.

[para 15] While I find that at the time of the breach, the Organization had not complied with section 34, I will not order that it do so as I am satisfied it has now taken appropriate steps to implement reasonable security measures that protect personal information

2. Did the Organization comply with section 35 of the Act (retention and destruction of information)?

[para 16] Section 35 of the Act states the following:

> *35(1) An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.*
>
> *(2) Within a reasonable period of time after an organization no longer reasonably requires personal information for legal or business purposes, the organization must*
>
> > *(a) destroy the records containing the personal information, or*
> >
> > *(b) render the personal information non-identifying so that it can no longer be used to identify an individual.*
>
> *(3) Subsection (1) applies notwithstanding any withdrawal or variation of the consent of the individual that the personal information is about under section 9.*

[para 17] The Organization has provided me with details regarding its retention policy at the time of the loss and the reasons for that policy. In initial submissions, the Organization states as follows:

> The human resources employee to whom the subject laptop was assigned was responsible for companywide human resource responsibilities. This employee had legitimate business purposes for maintaining this information including:
> • future recruiting and termination;
> • accounting;
> • tax;
> • legal; and
> • reporting purposes.
> [The Complainant] resigned in or around May of 2007. The laptop theft occurred on November 10 of 2014. Acosta's document retention practice at that time was to retain this information for a minimum of seven (7) years. Acosta is not aware of any specific legal or other requirement that this information be maintained for a different period of time.

[para 18] Further details were provided in the Organization's rebuttal submissions:

> Acosta has a large field force of product merchandisers who visit grocery stores and other retail outlets to ensure that the products of Acosta's clients are properly shelved, displayed, priced, advertised, etc. Acosta also employs personnel for specific in-store projects, such as resetting aisles in grocery stores. Acosta experiences frequent turnover in these field positions (and in its office administrative personnel, such as the Administrative Assistant

> position held by [the Complainant]) and will frequently employ the same person multiple times over a period of years. Therefore, Acosta has routinely retained employee information in order to source candidates for future positions and to retain work history information for persons who may leave Acosta and then apply for another position with Acosta in the future. Acosta takes the position that these are legitimate and necessary business and legal purposes to retain this information.

[para 19] The Organization has a burden to show that it met the requirements of section 35, of retaining information only for as long as reasonably required for legal or business purposes (P2006-011 at para 18).

[para 20] The Organization has told me it retained former employees' personal information for the purposes of re-recruiting them. However, without further information, it is impossible for me to make a determination whether information that would be needed for re-recruitment was being kept for that purpose was reasonable. For example, information about how often the employee information was actually used for re-recruitment, how long a period typically elapsed before an employee was re-recruited, and what proportion of past employees were actually re-hired, would enable me to perform the necessary balancing of this purpose against the privacy interests of former employees. In the absence of such information, the Organization has failed to satisfy me that the 7.5 year period for which it kept this former employee's personal information was reasonable within the terms of section 35.

[para 21] The Organization now has revised its retention policies. The following prefaces the schedule of the Organization's retention policy:

> **Policy for Retention of Employee Records**
>
> Acosta Canada Corporation ("Acosta") shall retain all paper and electronic records related to former associates of Acosta in accordance with the Retention Schedule attached hereto as Exhibit A (the "Retention Schedule"). After the applicable timeline specified in the Retention Schedule, all paper and electronic records related to such former associates shall be purged, deleted and/or destroyed, whether in paper or electronic format. The Human Resources Department shall have the authority to implement appropriate procedures related to the retention, review and purging of documents specified in the Retention Schedule. Documents shall be purged on a quarterly basis, except as may be otherwise noted in the Retention Schedule.

[para 22] I have been provided with a copy of the retention schedule and it is very detailed regarding employee information. It shows various retention periods for different types of records. For example, a Workers' Compensation claim record is kept for 10 years after the claim is closed unless the claim involves exposure to toxic substances which extends the term to 30 years. Compliance records are generally kept for a longer term than employment records. The retention schedule also directs documents be purged on a quarterly basis.

[para 23] Given the Organization has carefully considered appropriate periods for retention of information for various categories of employee information and has implemented policies to destroy that information once the retention period has lapsed, I am satisfied the Organization *now* has a policy regarding retention and destruction of personal information that is in compliance with section 35.

[para 24] I note the Organization has undertaken to confirm to the Complainant it has destroyed and deleted her personal information once this inquiry is concluded. I will order the Organization to provide me and the Complainant with confirmation the Complainant's personal information has been destroyed and is no longer retained by the Organization.

V. ORDER

[para 25] I make this Order under section 52 of the Act.

[para 26] I find the Organization was not in compliance with sections 34 and 35 of the Act at the time of the loss of the Complainant's personal information.

[para 27] I order the Organization to destroy the Complainant's personal information.

[para 28] I further order the Organization to notify me and the Complainant within 50 days of receiving this Order that it has complied with it.

Neena Ahluwalia Q.C.
Adjudicator