ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2012-02

April 30, 2012

ALBERTA TEACHERS' ASSOCIATION

Case File Number P1216

Office URL: www.oipc.ab.ca

Summary: The Complainant complained that the Alberta Teachers' Association (the "Organization") contravened the *Personal Information Protection Act* (the "Act") when it mistakenly mailed information regarding a downgraded reassessment of her teaching educational experience to another teacher. The mail was returned to the Organization approximately eight days after it had been sent out. The Organization admitted that it had improperly disclosed the Complainant's personal information. The Complainant argued that the Organization had not taken proper steps to prevent the mailing error in the first place, and had not taken proper steps to address it after it was discovered. The issue in the inquiry was whether the Organization had made reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of the Act.

The Adjudicator found that the misdirection of the mail was attributable to excusable human error, rather than any deficiency in security arrangements. Although the Complainant argued that there had been a serious failure on the part of a supervisor during what had been referred to as the Organization's "double-check" system for multiple mailings, the Adjudicator found that the involvement of the supervisor was an additional level of oversight not strictly required by section 34. It was sufficient for the first employee to process the mail, and his or her error was a rare mistake on the part of the Organization over the course of several years.

As for the steps taken by the Organization after the mailing error was discovered, the Adjudicator considered the nature and sensitivity of the Complainant's personal

information that had been improperly disclosed, and the risk of harm to the Complainant in the form of identity theft, humiliation or damage to reputation. He found that the information was not particularly useful for the purpose of identity theft, that it was unlikely that the teacher who had received the information would commit identity theft, and that it was unlikely that any other third party saw the Complainant's personal information and/or would commit identity theft. He also found that, although the misdirected personal information was relatively sensitive, its disclosure to a complete stranger was not likely to humiliate the Complainant or damage her reputation.

In view of the nature of the personal information and minimal risk of harm to the Complainant, the Adjudicator concluded that it was reasonable, in terms of security arrangements, for the Organization to ensure that the mail was returned to it. Contrary to the arguments of the Complainant, section 34 did not require the Organization to instruct the unintended recipient not to open the envelope and instead return it to the Organization sealed, did not require the Organization to contact the unintended recipient to determine whether anyone else had seen the contents of the mail, and did not require the Organization to notify the Complainant that her personal information had been mistakenly disclosed.

The Adjudicator accordingly concluded that the Organization made reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of the Act.

Statutes and Regulation Cited: AB: *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 1(1)(k) [formerly 1(k)], 2, 5(2), 34, 34.1, 34.1(1), 37.1, 37.1(1), 50(1), 50(5), 52 and 52(3)(a); *Personal Information Protection Amendment Act, 2009*, S.A. 2009, c. 50; *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003, s. 19.1(1).

Authorities Cited: AB: Orders P2006-008 and P2009-013/P2009-014; Decisions P2010-D-001 and P2011-D-001; Investigation Reports P2006-IR-005 and F2012-IR-01; *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner)*, 2011 ABQB 19. **CAN:** *Information and Privacy Commissioner v. Alberta Teachers' Association*, 2011 SCC 61**.**

Other Sources Cited: Office of the Information and Privacy Commissioner of Alberta, *PIPA Advisory #8 – Implementing Reasonable Safeguards* (Calgary: undated); Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner of British Columbia, *Getting Accountability Right with a Privacy Management Program* (Ottawa, Edmonton and Victoria: released April 17, 2012).

I. BACKGROUND

[para 1] On behalf of the Alberta Teachers' Association (the "Organization", "ATA" or "Association"), the Teacher Qualification Service ("TQS") assesses a teacher's

educational experience and prepares a Statement of Qualifications so that the teacher's employing school board knows where the teacher should be placed on the collective agreement salary grid for the purpose of setting the level of salary to be paid to the teacher.

[para 2] On April 17, 2008, the Complainant requested a reassessment of her educational experience. The Teacher Qualifications Committee met on April 25, 2008 and considered a number of requests for reassessment, including the Complainant's. A new Statement of Qualifications and Teacher Qualification Service Evaluation Summary, both dated May 6, 2008, were prepared. Together with a cover letter dated May 5, 2008 explaining the results of the reassessment, these items were mistakenly mailed to a third party in Red Deer rather than the Complainant in Edmonton. The third party was another teacher.

[para 3] Because the Complainant had been told to expect the results of her reassessment by regular mail by about May 2, 2008, she telephoned the Manager/Qualifications Secretary of the Teacher Qualifications Service (the "Qualifications Secretary") on May 5, 2008 to inquire about the reassessment. The Qualifications Secretary verbally advised the Complainant of the outcome. On May 8, 2008, the Complainant attended at the offices of the Organization at which time the Qualifications Secretary gave her a copy of the cover letter that set out the results of the Teacher Qualifications Committee's reassessment.

[para 4] Although the Complainant received a copy of the cover letter in person, she still did not receive, by May 15, 2008, a mailed copy of the cover letter, along with the Statement of Qualifications and Teacher Qualification Service Evaluation Summary. She therefore e-mailed the Qualifications Secretary on May 15 and 16, 2008. In an e-mail dated May 20, 2008, the Qualifications Secretary informed the Complainant that the results of her reassessment had been sent to an incorrect address and then returned to the offices of the Organization. The Qualifications Secretary wrote that the mail had been redirected to the Complainant on May 14, 2008. The Complainant received the mail on May 21, 2008.

[para 5] In a letter dated January 26, 2009, the Complainant complained that the Organization had contravened the *Personal Information Protection Act* (the "Act" or "PIPA") by mailing the information regarding the reassessment of her teaching educational experience to the third party. The former Commissioner authorized a portfolio officer to investigate and attempt to resolve the matter. This was not successful, and the Complainant requested an inquiry by correspondence dated June 4, 2009. By letter dated March 10, 2010, the former Commissioner advised the parties that an inquiry would proceed.

[para 6] In a letter dated March 19, 2010, the Organization objected to the inquiry proceeding, on the basis that the timelines and rules for extending a review under section 50(5) of PIPA had been breached by this Office, and on the basis that the nature of the

complaint did not warrant conducting an inquiry. The Complainant responded by letter dated March 30, 2010.

[para 7] In Decision P2010-D-001 issued April 27, 2010, the former Commissioner decided that the inquiry could proceed. The Organization brought an application for judicial review of that Decision. In *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner*, 2011 ABQB 19, dated January 12, 2011, the Court of Queen's Bench quashed Decision P2010-D-001, remitting the matter back to this Office and requiring it to be heard by a delegate of the Commissioner. The former Commissioner delegated the matter to me. I then received a round of submissions from the Organization and Complainant dated March 10, March 21, March 30 and April 30, 2011.

[para 8] In Decision P2011-D-001 issued May 5, 2011, I concluded that an inquiry should be conducted under section 50(1). However, this was subject to my decision as to whether the timelines and rules set out in section 50(5) had been breached, which I intended to make following a relevant upcoming decision of the Supreme Court of Canada.

[para 9] On December 14, 2011, the Supreme Court of Canada released its decision in *Information and Privacy Commissioner v. Alberta Teachers' Association*, 2011 SCC 61. That same day, I invited the parties to make any further submissions that they wished to make on the issue of whether this Office had lost jurisdiction to conduct an inquiry on the basis of alleged non-compliance with section 50(5) of PIPA. By letter dated December 19, 2011, the Organization withdrew its objection relating to the operation of section 50(5). I therefore no longer have to decide the foregoing issue.

[para 10] In order to address the merits of the Complainant's complaint, I held a hearing on April 20, 2012 at which each party made oral submissions. These were in addition to written representations regarding the merits of the complaint, as set out in the parties' material submitted to me previously. The Organization's Information and Records Manager, Privacy Officer and Archivist (the "Privacy Officer") attended the hearing as a witness; the Qualifications Secretary did not.

II. INFORMATION AT ISSUE

[para 11] The information that the Organization allegedly failed to protect under section 34 of PIPA is the Complainant's personal information contained in mail that was mistakenly sent to a third party. The mail consisted of a cover letter from the Organization to the Complainant, a Statement of Qualifications and a Teacher Qualification Service Evaluation Summary. The Complainant's personal information in the misdirected mail is described, in more detail, later in this Order.

III. ISSUE AND SUB-ISSUES

[para 12] The Notice of Inquiry, dated January 25, 2012, set out the following main issue:

> Did the Organization make reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of PIPA?

The Notice included the following four sub-issues, as adapted from concerns raised by the Complainant in her request for inquiry:

> Was the Organization's "double-check system" for multiple mailings sufficient for the purpose of complying with section 34?
>
> Did section 34 require the Organization to describe the envelope to the unintended recipient and instruct the recipient not to open it and instead return it to the Organization sealed?
>
> Did section 34 require the Organization, after receiving the envelope opened, to contact the unintended recipient to determine whether anyone else had seen its contents?
>
> Did section 34 require the Organization to voluntarily and immediately notify the Complainant of the misdirected mail?

The four sub-issues inform the main issue of whether the Organization made reasonable security arrangements to protect the Complainant's personal information, both before and after the mailing error. For instance, if the answer to the first sub-issue is "yes" and the answer to the other three is "no", then the Organization will have complied with section 34 of PIPA.

> Matters not relevant to the inquiry

[para 13] In Decision P2011-D-001, I stated that I would restrict the scope of the inquiry to the Complainant's concerns in relation to the misdirected mail. I explained that the inquiry would not address any possible concerns about a telephone conversation that the Complainant had with the Qualifications Secretary, or the propriety of the Organization's conduct in relation to matters that arose after the Complainant's initial complaint of January 26, 2009. The latter includes events surrounding the Organization's service of court documents on the Complainant in June 2010. I stated that the foregoing matters would only be considered to the extent that they raise facts relevant to the question of whether the Organization had proper processes in place to protect the Complainant's personal information in the misdirected mail. I also indicated that the inquiry would not address whether the Complainant is entitled to an apology from the Organization.

[para 14] In advance of the oral inquiry, the Complainant submitted an affidavit that she swore on February 28, 2012. In it, she disputes the accuracy of facts in relation to a request that she made for her TQS file in May 2008, as set out in an affidavit of the Organization's Privacy Officer sworn June 7, 2010. While the Complainant may be noting the discrepancies in order to challenge the credibility of the Privacy Officer, the Organization's response to the Complainant's request for her file is not the subject of this inquiry. The Complainant additionally notes that, when portions of her TQS file were hand-delivered to her, they were not in a sealed envelope. While I understand that the Complainant makes this point in order to argue that the Organization may not have properly protected other personal information of hers, only her personal information contained in the envelope that was misdirected to Red Deer is at issue in this inquiry.

[para 15] Portions of the Complainant's affidavit also dispute facts contained in an affidavit sworn on June 9, 2010 by the Qualifications Secretary. Again, the Complainant may be noting the discrepancies in order to challenge credibility, but the discrepancies themselves are generally not relevant to answering the main issue and sub-issues in this inquiry. For instance, the Complainant says that she did not telephone the Qualifications Secretary three times on a particular date, as alleged in the latter's affidavit, and she notes no record of any such calls in her TQS file. While the Complainant argues that this points to the inadequacy of the Organization's procedures for working with sensitive personal information, it has no bearing on the issue under section 34 of PIPA. If the Complainant did not make certain telephone calls and/or if the Organization did not keep a record of any telephone calls, this does not mean that it failed to protect the Complainant's personal information. Under section 34, the Organization has a duty to protect only personal information that is in its custody or under its control. Here, this consists of personal information of the Complainant that the Organization actually collected and recorded, not any of her personal information that it did not collect or did not record.

[para 16] In short, the content of the Complainant's affidavit of February 28, 2012 has little bearing on the matters to be addressed in this inquiry. The facts that she disputes in the affidavits sworn on behalf of the Organization are, as the Complainant herself often notes, not relevant in the first place.

IV. DISCUSSION OF ISSUE AND SUB-ISSUES

Did the Organization make reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of PIPA?

[para 17] Section 34 of PIPA 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 18] This case involves the TQS's misdirection of mail, intended for the Complainant in Edmonton, to another teacher in Red Deer. The fact that the mail was sent to the third party is not in dispute. The fact that the Organization did not describe the envelope to the unintended recipient, and did not instruct him or her not to open it but instead return it to the Organization sealed, is also not in dispute. The Organization further acknowledges that it received the returned mail opened, and that it did not subsequently contact the unintended recipient to determine whether anyone else had seen its contents. As will be discussed later in this Order, there is a disagreement over whether the Organization's eventual notice to the Complainant about the misdirected mail was immediate and voluntary.

[para 19] This inquiry addresses whether the Organization made reasonable security arrangements to protect against the risk of unauthorized disclosure of the Complainant's personal information (i.e., the mailing error in the first place) as well as to protect against the risk of further unauthorized disclosure and use of her personal information after the initial improper disclosure (e.g., to prevent additional third parties from seeing the mail or to prevent harm such as identity theft).

[para 20] At the oral hearing, the Organization's Privacy Officer explained that TQS provides its services on behalf of the Organization further to a memorandum of understanding between the Organization and Alberta Education, and that the TQS is staffed by employees of the Organization. The Organization does not dispute that it is responsible for the actions of the TQS. Even if TQS were not staffed by employees of the Organization, the Organization would still be responsible. Section 5(2) of PIPA states that, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with the Act.

General concepts: personal information, burden of proof and reasonableness

[para 21] Section 34 of PIPA requires an organization to protect what constitutes personal information. Under section 1(1)(k) of PIPA [formerly numbered section 1(k)], "personal information" means "information about an identifiable individual". Here, the misdirected mail contained the Complainant's personal information. The mail consisted of a cover letter, a Statement of Qualifications and a Teacher Qualification Service Evaluation Summary. The Complainant's personal information in the latter two items includes her full name, profession, educational institutions attended, the years that she attended them, the degrees and certificates conferred and their dates, and some details of the programs pursued (e.g., number of credit hours). The cover letter reveals that the Complainant requested a reassessment of her educational experience and indicates the outcome of the reassessment, as compared to the previous assessment. Together, the three items indicate how the TQS views the Complainant's educational qualifications for the purpose of teaching.

[para 22] With respect to section 34 of PIPA, an organization has the burden of proving that it made reasonable security arrangements to protect the personal information

that is 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/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 23] In deciding whether an organization made reasonable security arrangements under section 34, section 2 of PIPA must be borne in mind. 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, or not 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.

The Organization's general practices

[para 24] At the oral hearing, the Organization argued that it had reasonable security arrangements in place, in that it had implemented policies and procedures, had educated employees about them, and had ensured that employees complied with the policies and procedures to the extent that they were able to. The Organization's Privacy Officer testified that every new member of staff meets with her within a few days of employment, at which point she impresses upon them the need to comply with PIPA, including with respect to the protection of personal information. She noted that the Organization has taken steps to protect privacy that are consistent with those found in a recent publication released by this Office, being *Getting Accountability Right with a Privacy Management Program*. For instance, the Organization has high level executive support and a person expressly responsible for compliance with privacy legislation. The Organization argued that the totality of its policies and procedures demonstrates that it takes privacy and security of personal information very seriously.

[para 25] In my view, most of the foregoing points are not particularly relevant to this inquiry. An organization can have excellent and well-developed privacy policies and procedures, yet fail to make reasonable security arrangements in the circumstances of a particular incident or fall short in a specific area of its operations. I must consider the Organization's security arrangements, whether general or specific, insofar as they have a bearing on its efforts to prevent the misdirected mail in this case and to deal with that error after it occurred. Having said this, there are aspects of the Organization's general practices that are indeed relevant here, such as its procedure to investigate privacy breaches and conduct risk assessments.

[para 26] While the Organization noted its general or overall compliance with privacy requirements, the Complainant noted what she considered to be a pattern of mistakes and mismanagement on the part of the Organization in relation to her personal information. Throughout the material that she submitted, the Complainant points to various clerical or typographical errors on the part of the Organization. The Complainant argues that the Organization's clerical errors speak to its competency in the area of information management. However, the fact that an organization makes clerical errors does not, in and of itself, mean that the organization has failed to properly protect personal information under section 34, or that it otherwise contravened PIPA. In this inquiry, the only clerical errors that are relevant to the question of whether the Organization complied with section 34 are the one in relation to the placement of the mail in the wrong envelope, and another in relation to the Complainant's mailing address found in the cover letter setting out the results of her reassessment. The latter is relevant to the question of whether and to what extent the Complainant might have been subject to identity theft, as discussed later in this Order.

[para 27] At the oral hearing, the Complainant submitted that the Organization further demonstrated mismanagement of her personal information when the Privacy Officer provided a copy of her TQS file on school grounds without sealing the file in a secure package. I have already explained that this concern does not fall within the scope of the inquiry. Nonetheless, I take the Complainant's point to be that, if the Organization did not, in her view, properly secure her personal information when providing her TQS file, this might suggest that it did not properly secure her personal information in the course of mailing her reassessment. As will be discussed below, there is some uncertainty regarding the underlying events in this matter and perhaps, in the absence of clarity, the Organization's practices in other respects might assist in determining what actually occurred before and after the mailing error here. However, I do not find that I need to turn to other events in order to reach my conclusions in this inquiry. I will return to the facts below.

[para 28] At the oral hearing, the Complainant argued that the Organization "clearly" failed to make reasonable security arrangements given that its processes failed to prevent her personal information from falling into the wrong hands. The Organization responded that the fact that a privacy breach occurs does not mean that an organization failed to make reasonable security arrangements within the terms of section 34, as the standards will be applied by human beings, and privacy breaches will occasionally occur despite an

organization's best intentions. It cited an Investigation Report of this Office stating that it is not necessary that safeguards be "flawless" in order to be deemed reasonable (Investigation Report P2006-IR-005 at para. 14). The Organization also cited a publication of this Office, *PIPA Advisory #8 – Implementing Reasonable Safeguards*, which states (at page 2) that "reasonable" does not mean "perfect".

[para 29] The fact that the Complainant's personal information was improperly disclosed does not automatically or necessarily mean that the Organization failed to make reasonable security arrangements to protect it. I have explained that I must determine what steps were reasonable for the Organization to take, bearing in mind all of the relevant facts and circumstances.

1. Was the Organization's "double-check system" for multiple mailings sufficient for the purpose of complying with section 34?

[para 30] This sub-issue deals with the reasonableness of the Organization's security arrangements in view of its administrative practices when processing correspondence to be mailed. Reference has been made in the materials before me to a "double-check system" for multiple mailings. However, neither the Organization in its written submissions nor its witnesses in their affidavits describe the double-check system first-hand. Rather, they incorporate, by reference, facts described elsewhere.

[para 31] Specifically, the Qualifications Secretary attached, to her affidavit, a copy of a letter dated May 18, 2009, which was written to the Organization by the portfolio officer who investigated the Complainant's complaint to this Office. The Qualifications Secretary states that the letter accurately depicts the facts of this matter. The Organization's Privacy Officer also attached a copy of the letter to her affidavit, stating that the letter accurately describes the steps that she and TQS staff took to address the matter raised by the Complainant. In providing me with copies of the affidavits of the Qualifications Secretary and Privacy Officer (which were originally sworn for the purpose of the Organization's application for judicial review of Decision P2010-D-001), the Organization placed the facts, as set out in the portfolio officer's letter, before me for my consideration. The Complainant had already done likewise, having attached the same letter to her own request for inquiry and commenting on the facts set out in the letter.

[para 32] While the parties each placed the letter before me, I am not relying in any way on the analyses and conclusions of the portfolio officer, as I must separately and independently address the issues in this inquiry. As noted by the Court of Queen's Bench in *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner)*, a portfolio officer investigates the matter and attempts to negotiate or mediate a settlement between the parties, and it would generally be inappropriate for the Commissioner or an Adjudicator to consider materials that are settlement oriented (see para. 127). I am therefore disregarding most of the portfolio officer's letter. I am only referring to the portion setting out facts that the Organization adopts for the purpose of its submissions in this inquiry. These facts are not settlement oriented, in my view. Even if they are, I would respond that, because both parties relied on the facts set out by the portfolio

officer, both parties waived any settlement negotiation privilege to the extent that they relied on those facts.

[para 33] The portfolio officer's letter describes the relevant facts as follows:

> In this case, ATA advised me that a quantity of correspondence, including both letters and envelopes, were generated from a database containing personal information (e.g. mailing addresses). The result was a stack of labeled envelopes and a stack of letters, which were to be matched by an ATA staff member. The matched correspondence and envelopes were placed in a file, which was then provided to a supervisor. This stage of the process served as a "double-check" to ensure that letters were correctly matched to mailing envelopes. It was at this stage of the process that it was noted that a letter was incorrectly matched to the wrong envelope. Although the error was immediately apparent, and served to prevent a second mailing error, it appears that the complainant's letter (also matched to the wrong envelope) had already been sent, as it had been part of separate stack of letters reviewed by the supervisor the day before. In essence, while the complainant's letter was addressed correctly, it was inadvertently mailed in the wrong envelope.

[para 34] In view of the above facts, the Organization submits that the incident leading to the Complainant's complaint was in the nature of an isolated clerical error. It made the following argument in its submissions of March 10, 2011:

> Section 34 of PIPA requires that the Association take *reasonable* security arrangements. Clearly the Association took its duties under the Act seriously, attempted to protect the personal information of teachers and others, and did so almost invariably successfully over many years. The fact that a clerical error occurred which led to a misdirected piece of mail is no indication that the Association's security arrangements were not reasonable. Errors are an inevitable product of human activity and should not be taken as an indication that proper security measures are not in place.
>
> [Emphasis in original.]

The Organization's argument is essentially that the mishap here was due to rare and acceptable human error. In support of this argument, the Qualifications Secretary notes in her affidavit that the TQS has dealt with thousands of mailings to teachers. She states that, in her nearly five years with the TQS prior to the time that the mail intended for the Complainant was misdirected, she knows of only one other such mistake. At the oral hearing, the Organization's Privacy Officer testified that she has encountered only two mailing failures in the course of her six years of experience with the Organization.

[para 35] Conversely, the Complainant characterizes the misdirected mail as demonstrating a 50% error rate, in a short span of time, on the part of the supervisor responsible for ensuring that letters and envelopes are properly matched. While, overall, the TQS may rarely send mail to the wrong recipient, and the employee who initially prepares mailings may rarely mismatch letters and envelopes, the facts excerpted above indicate that the supervisor caught only one of two errors over the course of two days. In her submissions of March 21, 2011, the Complainant summarized her view as follows:

> While the concept of "human error" might be mildly appropriate to describe the stack matcher's malfunction it should certainly not be invoked to defend the apparent incompetence of the double-checker (a supervisor no less) whose specific responsibility was to prevent such mismatches.

The Complainant accordingly argues that the Organization's double-check system for multiple mailings was insufficient for the purpose of complying with its duty under section 34 of PIPA.

Lack of clarity regarding the facts

[para 36] The Complainant argues that the affidavits of the Qualifications Secretary and Privacy Officer are self-serving and factually incorrect. In her written material, she alleges a cover up following the Organization's violation of her privacy. She says, in particular, that parts of the affidavit of the Privacy Officer contain egregious errors as to how the Privacy Officer gave her access to her TQS file. At the oral hearing, the Privacy Officer acknowledged those errors, but I have already explained that the manner in which the Organization gave the Complaint access to her TQS file is not at issue in this inquiry. Still, the Complainant raises concerns about the sworn evidence and affirmed testimony of the Organization's witnesses, as well as concerns about the absence of the Qualifications Secretary at the oral hearing, in order to challenge the truth of the Organization's version of events, generally.

[para 37] I note that there are two versions of the facts, both emanating from the Organization, as to the nature of the mailing error that led to the improper disclosure of the Complainant's personal information. The excerpt reproduced above from the portfolio officer's letter, which contains facts subsequently incorporated by reference in the affidavit of the Qualifications Secretary, suggests that two sets of correspondence ended up in each other's envelopes. The Privacy Officer gave a different account at the oral hearing.

[para 38] During her cross-examination of the Privacy Officer, the Complainant asked for details regarding the Organization's procedure for matching correspondence and envelopes. The Privacy Officer was unable to give many details, as she was and is not involved in that process. However, she did recall that, during her discussions with the Qualifications Secretary, there was mention of two sets of correspondence being in the same envelope. In other words, the Red Deer teacher's assessment and the

Complainant's reassessment were in the same envelope sent to the teacher in Red Deer. Because the Complainant understood that another mailing error had been prevented, she asked what this other potential mailing error was. The Privacy Officer replied that she was not aware of any other mailing error that had been prevented in the course of the events giving rise to this matter. The Privacy Officer later indicated, in the course of the hearing, that the envelope in which the Complainant's correspondence was to be inserted was discovered by TQS staff without any correspondence to place into it.

[para 39] With this different version of the facts, the Complainant noted that an empty envelope would not have misdirected anyone's personal information, and so would not have been a second mailing error, at least not one that would lead to any privacy breach. She accordingly argued that the supervisor's failure to catch the only error that the first employee made when assembling the correspondence could be characterized as a 100% failure rate on the supervisor's part.

[para 40] Based on her understanding of the facts, the Complainant characterizes the supervisor's "primary role" or "main responsibility" as ensuring that the letters and envelopes were correctly matched and accordingly submits that he or she utterly failed. However, it had struck me as odd that a second individual would ensure that a first individual had properly matched letters to envelopes, as that task is not particularly complicated. When I sought clarity, at the oral hearing, as to why a supervisor would review the correspondence prepared by the first employee, the Privacy Officer replied that the supervisor reviews the assessments and reassessments for the purpose of knowing "have you got them all and are they ready to go". In other words, both an employee and supervisor appear to be involved so as to ensure that all of the assessments and reassessments in the particular batch are sent out. In short, my impression is that the supervisor does not literally make sure that each letter is matched up with the proper envelope before the envelope is stuffed. Indeed, the Privacy Officer indicated that this was not her impression either. Rather, the supervisor provides a more general review of the correspondence.

[para 41] The Complainant also has the impression that the mailing error was discovered around May 5 or 6, 2008 when the batch of correspondence was being sent out by the Organization over the course of two days. However, in her affidavit, the Qualifications Secretary clarifies that, while the mailing error occurred when assembling materials for mailing on May 6, 2008, a staff member of the TQS discovered the error on or about May 11, at which point the unintended recipient was contacted and asked to return the mail. I am not sure why it took approximately five days to discover the error but it was apparently discovered by the Organization first, and not the teacher in Red Deer who might have then alerted the Organization. The Privacy Officer testified that there was no mystery as to where the Complainant's reassessment had gone, given the sequence of the batch of correspondence generated from the computer database and therefore TQS staff's knowledge of the order in which teachers were sent the correspondence.

[para 42] The Qualifications Secretary might have confirmed or clarified the nature of the mailing error, and how and when it was discovered, if she had attended the oral hearing, but the Organization chose not to call her as a witness. In a letter dated March 7, 2012, the Complainant requested that I consider requiring the Qualifications Secretary to give testimony at the oral hearing. However, as set out in a letter dated March 15, 2012, I did not consider her potential testimony to be so crucial, for the purpose of deciding the issues in the inquiry, that I should exercise my discretion to summon her to attend. For reasons explained below, I do not need to ascertain the precise facts in order to reach my conclusion regarding the reasonableness of the Organization's mailing process as a security arrangement.

Conclusion regarding the Organization's mailing process

[para 43] For the purpose of deciding whether the Organization had reasonable security arrangements in place to guard against the possibility of misdirected mail, it does not matter whether the Complainant's envelope was discovered with another mismatched piece of correspondence or without any matching correspondence at all. It also does not matter exactly how the mistake was discovered. I attribute the improper disclosure of the Complainant's personal information to excusable human error, regardless.

[para 44] The mailing error in this case is properly characterized as one that occurred in a very rare instance, in view of the overall amount of correspondence sent out by the Organization, both over the years and in the course of the particular batch sent out around May 6, 2008. The Organization, like many, sends out a lot of correspondence. The Privacy Officer noted that the volume of mail that included the Complainant's reassessment was large, given the number of teachers seeking assessment of their educational experience following completion of their studies in April. As the mailing mistake was very rare, it falls within an acceptable range of human error and therefore does not mean that the Organization made unreasonable security arrangements under section 34 of PIPA.

[para 45] As set out as a general principle earlier in this Order, one of the factors to consider in determining whether an organization has complied with section 34 is the sensitivity of the personal information in question. The Complainant submits that her personal information in the misdirected letter consists of sensitive employment and educational information relating to the reassessment of her teaching qualifications. She says that the assessment "is a very serious document with a potential impact on a teacher's future".

[para 46] However, while the Complainant's personal information in the cover letter, Statement of Qualifications and Teacher Qualification Service Evaluation Summary was relatively sensitive, it was not so sensitive, in my view, as to require a second individual to review the matched envelopes and correspondence. It was sufficient to entrust a single employee of the Organization to place the items of correspondence in their proper envelopes. Indeed, I suspect that only a single employee did so in this case, even though a supervisor might subsequently have reviewed the assessments and reassessments in a

general way, or for a specific purpose other than literally ensuring that each set of correspondence and its envelope matched up correctly.

[para 47] The Organization noted that other organizations may not even have a second level of oversight when there are multiple mailings. I accept the Organization's explanation that the supervisor's involvement in this case was an added layer of protection that might guard against mailing errors, but that it was not strictly necessary for the purpose of complying with section 34. In short, whatever the "double-check system" might have been, it was better than nothing, given my view that a supervisor did not have to actually check each set of matched mail in the first place. Again, I think that one individual can successfully match correspondence to envelopes, regardless of the volume and even though there will sometimes be errors, as occurred in this case. If I were to say otherwise, I would be implying that every organization, at least for large batches of mail containing somewhat sensitive personal information, would need to have two people verify that each item of correspondence was properly stuffed in the right envelope. Such an administrative process would be unduly onerous.

[para 48] Having said this, there may be cases in which an organization might be required to have someone verify previously matched envelopes and correspondence, such as where the correspondence consists of extremely sensitive personal information about an individual and its disclosure to anyone other than that individual would cause him or her serious harm. However, that was not the case here. I can also envisage situations where an employee is prone to mismatching mail and an organization might therefore need another person to literally check each match. However, that was not the case here.

[para 49] Therefore, contrary to the argument of the Complainant, the mailing error at issue in this inquiry is not properly characterized as one on the part of the supervisor, which failed to remedy one of only two prior errors, or one of only one prior error, that the double-check system was intended to catch. It is properly characterized as a rare one on the part of the employee of the Organization who placed the mail intended for the Complainant in the envelope that went to the teacher in Red Deer.

[para 50] I conclude that the Organization's mailing process was reasonable for the purpose of making the security arrangements required by section 34 of PIPA.

[para 51] While the mailing error *per se* does not mean that the Organization contravened section 34, sub-issues remain about how the Organization dealt with the error once it was discovered. In her submissions of April 30, 2011, the Complainant argues that the Organization should have effective processes for dealing with the consequences of an inappropriate release of personal information after it has occurred. In other words, the Organization arguably contravened section 34 by failing to take proper steps to avoid or reduce the potential for consequences flowing from the fact that the mail intended for the Complainant was sent to a third party. As I noted earlier, section 34 of PIPA requires an organization to implement prudent and functional measures to mitigate reasonably foreseeable risks to the security of personal information.

2. Did section 34 require the Organization to describe the envelope to the unintended recipient and instruct the recipient not to open it and instead return it to the Organization sealed?

3. Did section 34 require the Organization, after receiving the envelope opened, to contact the unintended recipient to determine whether anyone else had seen its contents?

[para 52] I will address the above two sub-issues together, as they depend on essentially the same considerations, namely the nature and sensitivity of the Complainant's personal information that was misdirected and the potential consequences resulting from the Organization's failure to take the steps contemplated above.

[para 53] At the oral hearing, the Privacy Officer testified that TQS staff informed her that the Complainant's personal information had been mistakenly sent to the third party, and that they were working to get it back. She said that she then conducted a risk assessment, bearing in mind that staff knew where the mail had been sent, that the Complainant's personal information was not circulating in unknown places, and that the teacher in Red Deer was co-operating to return it. In the Privacy Officer's view, the personal information was not particularly sensitive and there was a minimal risk of harm to the Complainant. She noted that the mail did not contain a social insurance number or financial information, for instance.

[para 54] The Organization argued that the steps that it was required to take, following the privacy breach in this case, should be determined in reference to the investigation and risk assessment conducted by the Privacy Officer after the breach was discovered. In short, the Organization submits that the nature of the Complainant's personal information that was disclosed to the third party, and the circumstances of the disclosure, did not require it to take the above steps. It says that its Privacy Officer reasonably assessed the possibility of risk at the time, based on relevant information, and that her assessment should not be revisited as a result of what it views as mere speculation on the part of the Complainant as to possible harm. The Organization submits that it was sufficient, for the purpose of complying with section 34, that it ensured that the teacher in Red Deer returned the mail containing the Complainant's personal information.

[para 55] Given that the mail was sent to the third party on or about May 6, 2008 and was returned to the Organization on May 14, 2008, the Complainant submits that her personal information was unsecure for up to nine days and therefore could have been seen by anyone. However, at the oral hearing, the Organization's Privacy Officer indicated that the mail was sent by regular mail to and from Red Deer, meaning that part of the period between May 6 and May 14 included the time that it took for Canada Post to deliver the mail. I consider the Complainant's personal information to have been secure during this partial period. She does not allege that her personal information was insecure while being handled by Canada Post. While the Organization made oral submissions regarding the appropriateness of using the mail system in this case, the Complainant did

not complain about use of the mail system *per se*. Even following the privacy breach, she was content to have her reassessment redirected to her by regular mail.

Risk of identity theft

[para 56] Taking into account mail delivery of one or two days each direction, the Complainant's personal information was in the possession of the third party for roughly four to six days sometime between May 6 and 14, 2008. The Complainant fears that the teacher in Red Deer, or some other third party, may have been able to use her personal information contained in the misdirected mail to commit identity theft. In her initial complaint, the Complainant wrote the following:

> As you are aware, we are living in times of increasing identity theft. The highly confidential and sensitive career, employment, educational, and personal information that the TQS inappropriately released is precisely the kind of information that would support such a crime – in so doing, the ATA, through its TQS has exposed me to that very serious risk.

In her request for inquiry, the Complainant argued that the question of whether an organization has made reasonable security arrangements must be considered as a function of the seriousness of the potential adverse consequences.

[para 57] The Organization submits that the Complainant is overestimating the possibility of identity theft. In its submissions of March 10, 2011, the Organization wrote as follows:

> […] In particular, nothing in the Letter shows her [the Complainant's] complete mailing address since, through clerical error, the P.O. Box number is repeated and the postal code omitted. There is no street address which would allow for finding her postal code in a postal code directory. Without a postal code, the Complainant's mailing address is neither complete nor useable for the purposes of identity theft. Neither the names of the institutions she attended nor the dates she attended them could realistically further identity theft.
>
> The information is not particularly sensitive, nor is there a possibility of the information being misused because it does not appear to have a financial or other value. Even if the information had some theoretical or other value, there is no actual harm in this instance because the information was expeditiously returned to the Association by the unintended recipient, a fellow teacher, who was in contact with the Association. […]

The Organization added that, in its view, there is no possibility of the Complainant's personal information being misused, as the third party returned the mail to the Organization.

[para 58] In the excerpt above, the Organization notes that the cover letter that was misdirected to Red Deer did not contain the Complainant's complete mailing address. The Qualifications Secretary attached, to her affidavit, a copy of the cover letter dated May 5, 2008, containing the Complainant's P.O. Box number twice but no postal code. She states that this is the version sent to Red Deer, as well as the version provided to the Complainant in person on May 8, 2008. In a letter dated March 30, 2010 to this Office, the Complainant questioned whether the third party in Red Deer really received this version of the cover letter, as the cover letter that was subsequently mailed to the Complainant contained her P.O. Box and postal code. The Complainant submitted a copy of this version of the cover letter, also dated May 5, 2008.

[para 59] I find that the Organization, in fact, sent the third party the cover letter containing the Complainant's incomplete mailing address. I accept the evidence of the Qualifications Secretary, as found in her affidavit, which is to the effect that she corrected the Complainant's mailing address in the cover letter (but not the date) between the time that she received the original version of the cover letter back from the third party and the time that she mailed the second version to the Complainant. The Qualifications Secretary states that she "wanted to make sure that she [the Complainant] knew that we had corrected the erroneous address". At the oral hearing, the Complainant argued that, if the Qualifications Secretary wanted to assure her that the Organization was now working with her correct address, it should have advised her by telephone or e-mail rather than expect her to glean that fact from the altered cover letter. However, I find nothing wrong with the actions of the Qualifications Secretary in this regard. While the different versions of the cover letter and the fact that they bear the same date have caused some confusion, it was reasonable for the Qualifications Secretary to correct the mailing address on the cover letter before mailing it to the Complainant, rather than again send a letter known to contain an error.

[para 60] The parties' dispute over which cover letter was received by the teacher in Red Deer arose because it informs the question of how much of the Complainant's personal information was mistakenly disclosed. However, the fact that I have found that the letter did not contain the Complainant's complete mailing address does not affect my overall conclusions, in any event. I also do not make much of a disagreement between the parties, at the oral hearing, over whether or not the Complainant's degrees, certificates and their dates – as listed in her Statement of Qualifications and Teacher Qualification Service Evaluation Summary – are already ascertainable simply by contacting the educational institutions in question. Finally, the Organization noted that the Complainant's profession as a teacher is publicly available information, but I again find that this does not affect my analysis of the information in the misdirected mail and whether its disclosure subjected to the Complainant to possible identity theft.

[para 61] The reason that the Complainant's mailing address and the public availability of one or more of her educational and professional credentials are not particularly important is that it is the aggregate of information in the misdirected mail that may have subjected the Complainant to identity theft. Knowledge of only a mailing address or credential, whether publicly available or not, would not realistically assist an individual

to commit identity theft. Here, the Complainant's Statement of Qualifications and Teacher Qualification Service Evaluation Summary provided a complete list of her educational experience, including all of her degrees and certificates and the dates that they were conferred. It would not be very possible for a third party to amass this complete information, bit by bit, by calling various educational institutions. The information was conveniently presented to a potential identity thief in one fell swoop.

[para 62] As for whether the disclosure of the aggregate information in the misdirected mail was reasonably likely to give rise to identity theft, the Organization emphasizes that the recipient of the information was another teacher. The Privacy Officer testified that the teacher in Red Deer is bound by a Code of Conduct that requires teachers to treat one another fairly and with respect, and not to engage in activities that would dishonour their profession. She said that the teacher could be subject to a charge of professional misconduct if she refused to co-operate with the Organization and return the mail. The Privacy Officer further explained that, if a teacher commits a criminal offence, his or her teaching certificate may be revoked, which would affect his or her livelihood, so it is unlikely that the teacher in Red Deer would risk committing identity theft. The Privacy Officer said that she considered the teacher in Red Deer to be trustworthy. The risk of harm to the Complainant was, in her view, much lower than if the mail had been sent to an unknown member of the public, or an individual who was not another teacher.

[para 63] I agree that it was highly unlikely that the teacher in Red Deer would commit identity theft. Without meaning to imply that individuals belonging to certain professions are necessarily more trustworthy than other individuals, I would say that teachers tend to be law-abiding citizens, or at least not citizens prone to committing identity theft. The teacher in Red Deer was dealing with her professional body, and it is not likely that she would risk her professional status or open herself up to a criminal investigation by misusing the Complainant's personal information after being known to have received it. I accept the Organization's evidence that the teacher in Red Deer was co-operating to return the mail and was doing nothing suspicious that would cause concern.

[para 64] As for whether any other third parties had the opportunity to use the Complainant's personal information to commit identity theft, I also find this improbable. The far more likely fact scenario is that the teacher in Red Deer returned the mail immediately upon realizing that it was not intended for him or her, or very soon thereafter. While the teacher may have left the mail unattended in his or her residence, it would have been for a few days at most, given that the mail was sent to the teacher around May 6, received back by the Organization on May 14, and mail delivery accounted for part of the intervening period. The chances of another third party reviewing the correspondence in that short window, let alone memorizing or copying the information for the purpose of identity theft, are very small.

[para 65] Further, even if the teacher in Red Deer or another third party was prone to committing identity theft, the Complainant's personal information in the mail would not be particularly useful for that purpose. The Complainant's professional and educational information that was disclosed is far less useful than, say, a date of birth, social insurance

number, driver's licence number, personal health number, credit card number or bank account number. While the Statement of Qualifications included the Complainant's middle name, even her full name would not realistically enable identity theft without one of these other numbers that are routinely used for the purpose of identification, and therefore sought by identity thieves. While the Complainant noted, at the oral hearing, that the copy of her TQS file that she was given in May 2008 contained her social insurance number, the mail that was misdirected to Red Deer did not, and it is only the Complainant's personal information in the mail that is at issue in this inquiry.

[para 66] In Decision P2011-D-001, I raised the possibility that a third party might be able to use the Complainant's educational and employment information to impersonate her and obtain other information about her, for instance by telephoning or writing to her past educational institutions in an effort to learn other facts about her. At the oral hearing, the Complainant argued that the information was a starting point for identity theft, as a person could also call her pretending to be from one of her educational institutions. However, the evidence in this inquiry does not suggest any likelihood that someone could amass other information about the Complainant as a result of seeing the contents of the misdirected mail. As just explained, it is unlikely that the teacher in Red Deer would commit identity theft, and unlikely that other third parties saw the Complainant's personal information and/or would use it to commit identity theft.

[para 67] Even if the Red Deer teacher or another third party were prone to committing identity theft, I also find it unlikely that an individual could obtain useful information for that purpose by impersonating the Complainant or a representative of one of her educational institutions. Neither the educational institution, nor the Complainant herself, is likely to reveal additional personal information of the Complainant, and especially not the kinds of information desired by identity thieves, such as a social insurance number or credit card details. An educational institution would immediately become suspicious if someone purporting to be the Complainant requested identifying numbers or other information that the Complainant already knows, given that it is her own personal information. I also consider it unlikely that an identity thief would be able to extract additional personal information from the Complainant over the telephone or by sending an e-mail purporting to be from one of her educational institutions (i.e., by "phishing"). Given her strong objective to ensure that her personal information is not compromised, the Complainant is obviously savvy enough not to fall for such a manoeuvre. As noted by the Organization, virtually anything is possible when it comes to identity theft, but I must determine whether there is a reasonable possibility that someone might successfully use the Complainant's personal information in the misdirected mail to gather other facts about her for the purpose of identity theft. I consider this improbable.

Risk of humiliation or damage to reputation

[para 68] As I noted in Decision P2011-D-001, there does not actually have to be a risk that an individual will suffer a consequence such as identity theft in order for an organization to have failed to protect his or her personal information under section 34 of PIPA. Here, the nature of the Organization's breach of the Complainant's privacy by

allowing her personal information to be seen by a third party may, in and of itself, be serious enough to have required more stringent security arrangements.

[para 69] As explained earlier in this Order, the purpose of the Statement of Qualifications, which was disclosed to the teacher in Red Deer, was to indicate to a school board where the Complainant should be placed on a salary grid. I therefore considered whether it is possible that the third party deduced the Complainant's salary. At the oral hearing, however, the Organization's Privacy Officer clarified that the Statement of Qualifications assesses only a teacher's education for the purpose of salary, and not his or her experience teaching, which is an additional factor in determining salary.

[para 70] Still, the cover letter that was sent to the third party revealed the results of the reassessment of the Complainant's education, which reassessment was not favourable to her. I therefore considered whether the Complainant might have suffered any humiliation or damage to her reputation.

[para 71] The cover letter stated that the Teacher Qualifications Committee had decided to downgrade its earlier decision by awarding the Complainant no credit for her study at a particular educational institution. The letter stated that the institution was non-recognized and that no equivalencies from recognized institutions had been provided. At the oral hearing, the Organization argued that disclosure of the foregoing information was not reasonably likely to humiliate the Complainant or damage her reputation. The Privacy Officer explained that the cover letter and accompanying documentation simply indicated that the Complainant did not receive credit for a particular non-teaching program that she had submitted for consideration toward her educational experience. The Organization argued that the material did not show the Complainant in any negative light, or cast any aspersion on her qualifications or competence.

[para 72] Conversely, the Complainant said that disclosure of the results of her reassessment was embarrassing to her. She noted that a payroll representative of her employing school board, who routinely processes teachers' salaries, had never seen a downgraded reassessment. The Complainant submitted a copy of notes following a telephone conversation on May 21, 2008, in which she wrote that the payroll employee "expressed shock and said she had never seen this before". The Privacy Officer countered that an assessment or reassessment that does not credit certain educational experience for the purpose of salary may not occur every day, but it is not a rarity.

[para 73] In my view, the results of the reassessment of the Complainant's educational experience might be seen as placing her in a negative light, in that they revealed that she had been unsuccessful in having the previous decision of the TQS reversed. The cover letter stated that the Committee had decided to downgrade the previous decision, meaning not only that the Complainant had lost in her attempt to get a better assessment, but had actually obtained an even more unfavourable one. While the Complainant's salary could not be deduced from her educational experience alone, the reassessment indirectly revealed that her salary might be decreased, given that part of her educational

experience had been discounted for the purpose of determining salary. The Organization argued that an individual without the necessary knowledge of TQS rules would not understand the implications of the Complainant's reassessment. However, it was not just an ordinary member of the public who received her reassessment; it was another teacher going through the same process. Finally, the reputation of the Complainant might have been damaged to the extent that someone reading that she attended a "non-recognized" institution might think that the institution was, in some way, inferior. I acknowledge that the program attended by the Complainant at the non-recognized institution was not a teaching program, but I still think that a third party could negatively interpret the results of the reassessment, and even if that negative interpretation would be unwarranted.

[para 74] While I find that the Complainant's personal information that was misdirected to Red Deer was of a type that might be seen as causing her some humiliation or some damage to reputation, the nature of the recipient of the information leads me to conclude the opposite, in the end. The Complainant notes that, while the third party in Red Deer was another teacher, he or she was a complete stranger. The fact that the third party was a stranger to the Complainant, and did not work with her, militates against a finding that the Complainant suffered a serious breach of privacy resulting in any humiliation or damage to reputation. It would have been far more serious, in my view, if a co-worker or acquaintance of the Complainant learned the results of her reassessment. A complete stranger would presumably have no interest whatsoever in the Complainant's educational credentials, salary or reassessment, and would not have any desire or opportunity to disseminate that information, for instance as might occur by way of office or school gossip.

[para 75] Given the foregoing, and notwithstanding the relative sensitivity of the Complainant's personal information in the misdirected mail, I find that the risk that the Complainant would be humiliated or suffer damage to reputation, as a result of the disclosure to the third party in Red Deer, was minimal. Bearing this in mind, as well as my finding that the risk of identity theft was also small, I now turn to the two sub-issues above.

Conclusion regarding the Organization's contact with the third party

[para 76] An indication to the teacher in Red Deer not to open the envelope would have been a security arrangement by the Organization, within the terms of section 34 of PIPA, to protect against unauthorized disclosure of the Complainant's personal information to the teacher or any other third party. If the teacher had not opened the envelope, the Complainant's personal information would not have been disclosed. However, because the risk of identity theft, humiliation or damage to reputation was minimal even if the third party opened the envelope, section 34 did not require the Organization to instruct him or her not to open it and instead return it to the Organization sealed. As noted earlier, section 2 states that the standard to be applied is what a reasonable person would consider appropriate in the circumstances. I find that the Organization met this standard by asking the third party to return the mail, even though he or she was not told to return it unopened.

[para 77] In a different case, section 34 might reasonably require an organization to expressly ask for the return of misdirected mail unopened, assuming that there is an opportunity to do so in time. I referred earlier to the disclosure of identification numbers that are typically used for the purpose of identity theft, and to situations where an individual might suffer mental anguish if a closely connected third party were to learn sensitive personal information about the individual. Depending on the contents of misdirected mail and who the unintended recipient is, an organization might have to take steps to mitigate the possibility of the contents actually being seen.

[para 78] As for whether the Organization was required, by section 34, to follow up with the third party in Red Deer after the mail was returned opened, so as to determine how long the mail was in the possession of the third party and whether anyone else had seen its contents, the Organization was not so required. Such a step is arguably not contemplated by section 34 at all. Once the Complainant's personal information was seen by the teacher in Red Deer or anyone else, the disclosure already occurred and there was nothing that the Organization could do to protect against further disclosures or uses of the Complainant's personal information. To put the point differently, once the Complainant's personal information in the misdirected mail was memorized, copied or otherwise retained by the teacher in Red Deer or any other third party, this personal information was no longer in the custody or control of the Organization, as set out in section 34, and the Organization therefore had no ability to protect it. The damage would have already been done, so to speak.

[para 79] Even if a follow-up call to the teacher in Red Deer might have somehow prevented a further disclosure or use of the Complainant's personal information, section 34 would still not have required the Organization to take that step, again because of the minimal risk of identity theft, humiliation or damage to reputation. If the mail intended for the Complainant was accessible to various third parties within the residence of the teacher in Red Deer and over the course of several days, it is unlikely that any of those third parties could use the personal information in the mail to commit identity theft, even assuming that they were prone to do so. It was also unlikely that the Complainant would be embarrassed or suffer damage to reputation if any of those third parties learned the results of the Complainant's reassessment. Again, these complete strangers would not be interested in the information and/or would not have any desire or opportunity to disseminate it in a way that would embarrass the Complainant or damage her reputation.

[para 80] At the oral hearing, the Complainant noted that the Organization simply cannot be certain that others apart from the teacher in Red Deer did not view the misdirected mail. She is concerned that, even today, she still does not know how many sets of eyes have fallen on her personal information. The Complainant said that she was not accusing the teacher in Red Deer of any wrongdoing; it is just that she does not know what happened after her personal information was mistakenly disclosed. She argued that, if the Organization had simply instructed the third party not to open the envelope, she would not be left wondering about any of the foregoing.

[para 81] However, section 34 of PIPA does not require an organization to comprehensively investigate all privacy breaches and conclusively determine what happened in every respect. What constitutes reasonable security arrangements depends on the magnitude of risk and the likelihood that it will materialize. An individual whose personal information has been compromised will no doubt want the utmost to be done to prevent any possibility of harm whatsoever. However, as noted by the Organization, the standard required by section 34 must be viewed objectively, not subjectively through the eyes of the individual whose personal information is at issue. Indeed, this is the standard effectively set out in section 2.

[para 82] I conclude that, due to the nature of the Complainant's personal information that was disclosed and other relevant circumstances suggesting that the risk of identity theft, humiliation or damage to reputation was minimal, the Organization was not required to describe the envelope to the third party and instruct that it not be opened, and was not required to contact the third party to determine whether anyone else had seen its contents. In order to make reasonable security arrangements as required by section 34 of PIPA, it was sufficient for the Organization to take steps to ensure that the mail was returned to it in a timely manner.

4. Did section 34 require the Organization to voluntarily and immediately notify the Complainant of the misdirected mail?

[para 83] The Complainant argues that the Organization should have voluntarily and immediately notified her that her personal information had been mistakenly disclosed to a third party, rather than only peripherally after she contacted the Organization looking for the expected mail containing the results of the TQS's reassessment of her educational experience. As noted earlier, the Organization discovered the mailing error on or about May 11, 2008, and the Qualifications Secretary informed the Complainant about the error in an e-mail on May 20, 2008. While the Organization argues that this shows that it voluntarily informed the Complainant, the Complainant's point is that she should have been informed in a more formal and proactive manner. The Applicant questions why it took the Organization several days.

[para 84] At the oral hearing, the Privacy Officer testified that, on learning about the misdirected mail, she instructed TQS staff to notify the Complainant. However, she said that notice was given as a courtesy, not due to any particular risk. The Organization submits that, in any event, the notice was timely and it places no importance on the fact that the notice came in the form of an e-mail replying to an e-mail from the Complainant. The Complainant countered that TQS staff had a few opportunities to advise her of the disclosure in the course of her communications with them, but chose not to do so until May 20. She believes that this is not consistent with a direction from the Privacy Officer that they inform her, although I note that the Privacy Officer testified that she did not specify when or how the notice should be given.

Conclusion regarding notice to the Complainant

[para 85] Again, section 34 of PIPA requires an organization to make reasonable security arrangements to protect personal information. Here, it would have been very easy for the Organization to contact the Complainant on or about May 11, 2008 when it realized that her personal information had been mistakenly sent to a third party. However, in reference to section 2, I find that a reasonable person would not consider that the Organization, in the circumstance of the case, should have formally or proactively informed the Complainant of the privacy breach. The specific obligations of the Organization, in order to meet its duty under section 34, are a function of the sensitivity of the Complainant's personal information and the risk of harm to her as a result of the improper disclosure. As already explained in this Order, there was an insufficient risk of identity theft, humiliation or damage to reputation so as to require the Organization to notify the Complainant.

[para 86] Further, I fail to see how the Complainant, in knowing that her personal information had been improperly disclosed to the third party, could take steps to prevent further uses or disclosures of that particular personal information. When I asked the Complainant, at the oral hearing, to explain to me what would have been accomplished by way of mandatory and proactive notice, in terms of mitigating the risk of harm to her, she could not say. In my view, notice would not have served to guard against further unauthorized uses or disclosures of the Complainant's personal information. I have addressed in this Order whether it was likely that the information at issue would be used to commit identity theft, and have found otherwise. I have addressed whether it was likely that the information at issue would be further disclosed in a manner that might humiliate the Complainant or damage her reputation, and have found otherwise. Notice to the Complainant would not have usefully diminished risks that were already minimal. Contrary to what might occur in a different case, there was no identification number that was mistakenly disclosed that the Complainant could take steps to change. The Complainant did not need to know about the disclosure in order to counter any tarnish to her reputation, as the disclosure of her personal information to a complete stranger in a different city did not give rise to any reasonable concern in this regard.

[para 87] At the oral hearing, the Complainant further noted that the Organization's e-mail of May 20, 2008 did not inform her of the method of delivery or the address to which her personal information had been mistakenly sent. It also did not indicate the dates that the misdirected mail had been sent and returned, or that it had been opened by the third party. All of these questions have essentially now been answered, including the address where her personal information was sent in that the Complainant knows that it was Red Deer. However, for the reasons just set out, it was not necessary for the Organization to provide any of the foregoing information to the Complainant in order for it to comply with section 34.

[para 88] At the oral hearing, the Complainant noted that, in a different matter involving a loss of personal information, Edmonton Public Schools promptly and proactively notified all affected employees both by letter and e-mail, prepared a question

and answer table to assist employees, and even informed employees how to contact this Office. She says that these steps are in stark contrast to how the Organization approached the violation of her privacy. However, the matter involving Edmonton Public Schools was very different. In particular, the personal information at issue was far more extensive and sensitive than in the present inquiry. A USB Stick had been lost and it contained the personal information of over 7,000 individuals, including copies of their resumes, driver's licenses, first page of passports, birth certificates, injury forms, payroll and pension correspondence, performance evaluations and police criminal records check reports (See Investigation Reports F2012-IR-01 at paras. 1 and 22). As noted by the Organization in this inquiry, Edmonton Public Schools also failed to follow its own policies. For instance, it did not ensure that the USB stick was encrypted or password protected (see paras. 31 to 36).

[para 89] I conclude that the Organization was not required to notify the Complainant that her personal information had been disclosed to the third party in order to comply with section 34 of PIPA.

[para 90] Having said this, it is generally good practice for an organization to notify an individual when his or her personal information has been mistakenly disclosed to a third party, or otherwise compromised or left unsecure, even if this is not required by section 34. The Complainant has concerns that such privacy breaches would otherwise go undiscovered. I would add that an individual is generally in the best position to determine whether an erroneous disclosure of his or her personal information has the potential for consequences, and generally in the best position to take steps to prevent those consequences, particularly where the organization no longer has control over the information. However, I can only find or order what PIPA requires an organization to do, and I find that it did not require the Organization to notify the Complainant of the misdirected mail in this case.

Amendments to PIPA in 2010

[para 91] On May 1, 2010, two new sections 34.1 and 37.1 of PIPA came into force by virtue of the *Personal Information Protection Amendment Act, 2009*. The amendments set out a regime in relation to an organization's obligation to provide notification following the loss or compromise of personal information. Sections 34.1 and 37.1 did not exist at the time of the Organization's alleged contravention of section 34 in May 2008, so the Organization was not subject to the requirements of those provisions. However, for reasons explained below, I consider their enactment relevant to determining what section 34 of the PIPA required of the Organization by way of reasonable security arrangements to protect the Complainant's personal information in May 2008. In short, the enactment of the new provisions confirms my conclusion that the Organization was not required to notify the Complainant that the mail intended for her was mistakenly sent to a third party.

[para 92] Sections 34.1 and 37.1 read, in part, as follows:

> *34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.*
>
> *…*
>
> *37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure…*

[para 93] Section 34.1(1) requires an organization to provide notice to the Commissioner of any incident involving the disclosure of personal information where a reasonable person would consider that there exists "a real risk of significant harm" to an individual as a result of the disclosure. In turn, section 37.1(1) authorizes the Commissioner to require the organization to notify the individual. Under section 19.1(1) of the *Personal Information Protection Act Regulation*, which likewise came into force on May 1, 2010, the notification must be given directly to the individual, and it must include a description of the circumstances of the disclosure, the date on which the disclosure occurred, a description of the personal information involved in the disclosure, a description of any steps the organization has taken to reduce the risk of harm, and contact information for a person who can answer, on behalf of the organization, questions about the disclosure.

[para 94] Sections 34.1 and 37.1 were certainly not enacted in order *to reduce* the responsibilities of an organization following the loss of, unauthorized access to, or disclosure of, personal information. Rather, they were enacted *to strengthen* the obligations of organizations in this regard, and therefore improve security with respect to personal information. In other words, the amendments may be taken to set out no less stringent a regime for the protection of personal information than existed at the time of the Organization's alleged contravention of section 34.

[para 95] Taking this line of analysis further, if the Organization had sent the Complainant's personal information to the third party in Red Deer today, the new regime would not have required it to notify the Commissioner and, in turn, the Complainant. For all of the same reasons explained earlier in this Order, the erroneous disclosure of the Complainant's personal information did not involve a real risk of significant harm, as set out in sections 34.1(1) and 37.1(1). If the Organization would not have been required to notify the Complainant under the more stringent regime, it was not required to do so when only section 34 of PIPA existed to protect the security of personal information.

V. ORDER

[para 96] I make this Order under section 52 of PIPA.

[para 97] I find that the Organization made reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of PIPA. Under section 52(3)(a), I confirm that the Organization performed its duty under section 34.

Wade Riordan Raaflaub
Adjudicator