Order P17-01

CONSTRUCTION MAINTENANCE AND ALLIED WORKERS LOCAL 2423

Carol Whittome
Adjudicator

February 6, 2017

CanLII Cite: 2017 BCIPC 05
Quicklaw Cite: [2017] B.C.I.P.C.D. No. 05

Summary: A complainant alleged that the organization had disclosed his personal information contrary to PIPA after a document containing organization member names and their corresponding debts to the organization was placed in a public workplace location. The complainant also alleged that the organization failed to protect the personal information in its custody or control. The adjudicator found s. 18(1)(g) of PIPA did not authorize the organization to disclose the personal information, and the organization did not protect the personal information in its custody and control, contrary to s. 34 of PIPA.

Statutes Considered: *Personal Information Protection Act*, ss. 2, 4, 18(1)(g) and 34.

Authorities Considered: B.C.: Order P15-01, 2015 BCIPC 20 (CanLII); Order P05-01, 2005 CanLII 18156 (BC IPC); Order P09-01, 2009 CanLII 38705 (BC IPC); Order P11-02, 2011 BCIPC 16 (CanLII); Order P12-01, 2012 BCIPC 25 (CanLII); Order P13-02, 2013 BCIPC 24 (CanLII); Order P06-04, 2006 CanLII 37938 (BC IPC); Order P06-03, 2006 CanLII 32981 (BC IPC); Investigation Report F06-01: *Sale of Provincial Government Computer Tapes Containing Personal Information*, 2006 CanLII 13536 (BC IPC); OIPC's *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*.

Authorities Considered: Federal: PIPEDA Incident Summary #10.

INTRODUCTION

[1] This hearing arises from a complaint made by an individual alleging that his personal financial information was disclosed by the Construction Maintenance and Allied Workers, Local 2423 (the "Union") contrary to the *Personal Information Protection Act*.

[2] In January 2015, the complainant found a document that had been left in the workplace lunchroom, which outlined the amount of money the complainant (amongst others) owed to the Union.

[3] The complainant sent a letter to the Union alleging that it had not kept his personal financial information confidential. On March 4, 2015, the Union responded to the complainant, stating that section 18(1)(g) of *Personal Information Protection Act* ("PIPA") authorized the disclosure.

[4] On May 5, 2015, the complainant requested that the Office of the Information and Privacy Commissioner ("OIPC") review the Union's response to the complaint. Mediation did not resolve the issues and the applicant requested they proceed to a written hearing.

ISSUES

[5] The issues to be decided in this hearing are as follows:

1. Whether section 18(1)(g) of PIPA authorized the Union to disclose the complainant's personal information without his consent in order to collect a debt; and

2. Whether the Union protected the personal information in its custody or control, pursuant to section 34 of PIPA.

[6] Section 51 of PIPA sets out the burden of proof in the hearing process, but it does not address the burden required for this type of complaint.[1] It is therefore in the interests of both parties to provide evidence and arguments to support their positions.[2]

[1] Section 51 of PIPA only pertains to specific situations, none of which are relevant in this case.
[2] Order P15-01, 2015 BCIPC 20 (CanLii), para. 3.

DISCUSSION

Background

[7] The Union is a trade union within the meaning of the *Labour Relations Code* and is certified to represent certain employees of School District No. 78.[3] As such, it is an "organization" and subject to PIPA.[4]

[8] The Union engaged in a strike pursuant to the *Labour Relations Code* and provided its members with strike pay, on the condition that the members would repay it once the strike had concluded.[5]

[9] The complainant is employed by School District No. 78, and is a member of the Union. He received strike pay, which he agreed to pay back.[6]

[10] As of January 2015, approximately 125 members had made either partial or no repayment. The Union's Secretary-Treasurer prepared a list of members and their corresponding outstanding payments and emailed it to 12 individual Union members in the various School District's departments.[7]

[11] As noted above, the complainant found a document that had been left on a table in the lunchroom at his workplace, which listed approximately 125 names and the amount of strike pay that each individual, including the complainant, owed to the Union. The Union asserts that s. 18(1)(g) authorized the disclosure and it has, therefore, not contravened PIPA.

[12] There is no evidence or argument before me as to how the printed list ended up in the public lunchroom. However, the Union concedes that the information was personal information and that the Union disclosed it without consent.[8] In its argument, the Union does not appear to differentiate between the disclosure of the information via email to the 12 individuals and the disclosure of the information via a document left on a lunchroom table at one particular location.

[13] Also, according to a letter from the Union to the complainant, "each department representative [the 12 people who received the email] was asked to make their co-workers aware of the document so that they might check their individual balances" and notes that if the list was posted "it was at the sole discretion of the contact person at the location…."[9] Therefore, I take from the

---

[3] Union submissions, para. 1.
[4] PIPA, ss. 1 (definition of "organization") and 3.
[5] Union submissions, para. 3.
[6] Union submissions, para. 1. The complainant does not dispute this assertion in his submissions.
[7] Union submissions, para. 4.
[8] Union submissions, para. 7.
[9] Complainant submissions, para. 4, document 1. Note: the complainant did not provide affidavit evidence; rather, he provided submissions and five documents in support of those submissions. The Union did not make any submissions regarding the content of these documents.

Union's submissions and the evidence before me that the Union concedes that one of its representatives was responsible for the document being printed out and left in a public location.

Section 18(1)(g) – disclosure without consent to collect a debt

[14] Section 18(1) sets out the circumstances where an organization can disclose an individual's personal information without their consent. The relevant section in this case states:

> 18 (1) An organization may only disclose personal information about an individual without the consent of the individual, if
>
> …
>
> (g) the disclosure is necessary in order to collect a debt owed to the organization or for the organization to repay an individual money owed to them by the organization,

[15] "Personal information" is defined in s. 1 of PIPA, as follows:

> "personal information" means information about an identifiable individual and includes employee personal information but does not include
>
> (a) contact information, or
>
> (b) work product information;

[16] The term "necessary" is not explicitly defined in PIPA. As well, neither party referred me to, nor am I aware of, any OIPC orders that deal with the definition of "necessary" within the particular context of s. 18 (*i.e.*, where disclosure without consent is permitted in certain circumstances).

[17] However, previous orders dealing with other sections of PIPA have considered the meaning of the word "necessary" and, in my view, the principles in those orders are relevant to this situation.[10]

[18] In Order P09-01, former Commissioner Loukidelis held that in order to be "necessary", the collection, use or disclosure must be more than "simply convenient" to achieve the purpose, although this does not mean that the collection, use or disclosure of the personal information must meet "a strict standard of indispensability."[11]

---

[10] See, for example, Order P05-01, 2005 CanLII 18156 (BC IPC), paras. 67 and 78; Order P09-01, 2009 CanLII 38705 (BC IPC), paras. 34 – 42.
[11] Order P09-01, 2009 CanLII 38705 (BC IPC), para. 34 and 40.

[19] Another adjudicator elaborated on this in a subsequent order, and stated the following:

> … As interpreted in Cruz Ventures, "necessary" in this context does not mean "indispensable", in the sense that it is not possible to supply the product or service without the information. However, the organization must demonstrate that obtaining the information is more than merely convenient or of some possible future use. It must be integral to the provision of the product or service, in that it plays a significant role in enabling the organization to achieve the purpose for which the information is collected. The organization's demonstration of necessity will be carefully scrutinized in light of the purpose of PIPA. …[12]

[20] Orders P05-01 and P09-01 set out some of the factors to consider when determining whether the test of "necessary" has been met. I summarize these as follows:

- sensitivity of the information;
- amount of personal information disclosed;
- manner/scope of disclosure;
- effectiveness of disclosure in achieving the purpose; and
- whether there are less privacy-intrusive means of achieving that purpose.[13]

[21] Of course, this list is not exhaustive and other factors may be relevant depending on the particular circumstances of the situation.

[22] While the Union must establish that the disclosure was "necessary" in order to prove that s. 18(1)(g) applies, it must also establish that a reasonable person would consider the disclosure to be appropriate in the circumstances. That is because reasonableness is an overarching standard throughout PIPA.

[23] Section 4 of PIPA explicitly requires organizations to consider the reasonableness of their actions in meeting their responsibilities under the legislation:

> 4(1) In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.

[24] The purposes of PIPA also explicitly refer to the concept of reasonableness. Section 2 states:

---

[12] Order P11-02, 2011 BCIPC 16 (CanLII), para. 78.
[13] Order P05-01, 2005 CanLII 18156 (BC IPC), particularly para. 89; Order P09-01, 2009 CanLII 38705 (BC IPC), particularly paras. 35, 38 and 40 – 42.

> 2 The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[25] In Order P12-01, former Commissioner Denham provided a list of non-exhaustive factors to consider when determining the reasonableness of an organization's actions. That list mirrors the factors set out in Orders P05-01 and P09-01.[14]

[26] Therefore, the same factors are considered in both the "reasonable" and the "necessary" test. However, there is a different threshold to meet for each test. Reasonableness requires a consideration of whether a reasonable person would consider the disclosure appropriate in the circumstances; whereas, necessity requires a consideration of how integral the disclosure is in order to achieve the purpose sought. Again, an organization does not have to establish that the disclosure is "indispensable" but it does have to establish that the disclosure was integral to achieving the purpose sought, which requires evaluating whether it plays a "significant role" in achieving that purpose.

[27] Since the factors in both tests are the same, I will consider both the reasonableness and the necessity of the disclosure at the same time in my analysis.

Complainant's position

[28] The complainant submits that the Union has his "civic and electronic addresses", as well as his workplace email address, and it could have contacted him personally regarding the repayment. He says that it was not necessary for the Union to send out an "omnibus email" of all of the members' outstanding debt. Rather, he surmises that it was simply "expedient and convenient" for the Union to do so and that this does not meet the threshold of necessity required by PIPA.[15]

[29] The complainant also submits that it is "not reasonable to argue that it was necessary to compile all of the members owing a debt onto a list and email it on January 19, 2015 throughout the school district."[16] He notes that, according to the email, the debt did not have to be fully repaid until June 2015.[17] Even then the Union's deadline was not rigidly fixed and there was an option to extend it, according to another document outlining the strike pay the complainant received.[18]

---

[14] Order P12-01, 2012 BCIPC 25 (CanLII), paras. 123 – 166, cited in Order P13-02, 2013 BCIPC 24 (CanLII), para. 48.
[15] Complainant submissions, para. 3.
[16] Complainant submissions, para. 4.
[17] Complainant submissions, para. 4, document 1.
[18] Complainant submissions, para. 4, document 2.

[30] In an email he sent to the Union, the complainant noted that the Union had never set a deadline for repayment until the Union sent out the January 2015 email.[19] He further stated that he "failed to comprehend how it could be possible to find it a necessary act to collect a debt owed when parameters were never established by the Union."[20] The complainant submits that regardless of the exact deadline for repayment, "it was not necessary to violate the privacy of over 125 of its members in January of 2015."[21]

[31] The complainant did not make specific submissions regarding the reasonableness of the Union's disclosure, but based on what he does say, I understand him to be arguing that the disclosure was neither necessary nor reasonable in these circumstances.

Union's position

[32] The Union states that the strike money that the members received came from union dues, which all members pay. Furthermore, the repaid money would be used to further the purposes and goals of the Union, including future strikes, administration of the collective agreement, arbitration expenses and training.[22]

[33] The Union submits that the purpose of circulating the list of outstanding payments was to bring to its members' attention the amounts owed and the timeframe to repay the monies. It further states that, given the large number of individuals involved, it was "not inappropriate to provide a single list", particularly since "everyone knew that all of the employees had received strike pay and were under an obligation to make repayment."[23] Therefore, it submits that it was necessary to disclose the names and amounts owed in order to collect the debts.[24]

[34] The Union also submits that Union members would consider it reasonable for other Union members to receive information as to the outstanding payments, since those who received strike pay did so on the understanding that it would be repaid. This information, it submits, established the "joint liability" of members, and it was in every member's interest to have a clear understanding of what was owed to the organization.[25]

[35] The organization also submits that it was not a secret that strike pay was disbursed and that members had an obligation to repay that money. It believed "that members of the union could use moral suasion in order to convince other

[19] Complainant submissions, para. 4, document 5. The Union did not dispute this in its reply submissions, other than to submit that the complainant's concern about the "timing of the notice" is irrelevant to the question of whether it complied with s. 18(1)(g): Union submissions, para. 8.
[20] Complainant submissions, document 5.
[21] Complainant submissions, para. 4.
[22] Union submissions, para. 10.
[23] Union submissions, para. 15.
[24] Union submissions, para. 16.
[25] Union submissions, paras. 7, 9 and 11.

members to make repayment" and that this was an appropriate method to use to collect the money owed.[26]

Analysis, s. 18(1)(g)

[36] In considering s. 18(1)(g) in this situation, the Union concedes that the information in question is personal information within the meaning of PIPA and that disclosure without consent did occur.[27] Further, the complainant does not disagree that he owed a debt to the Union at the time the January 2015 email was sent.

[37] The email that led to the wider disclosure in the lunchroom contained Union member names, as well as the amount of strike pay they were paid and still owed to the Union. I find that this is personal information, as defined by PIPA. Therefore, the only question is whether the disclosure was "necessary" to collect the outstanding debt and whether a reasonable person would consider the disclosure appropriate in the circumstances.

[38] As noted above, I consider the factors outlined in Orders P05-01, P09-01 and P12-01 to be useful in determining whether it was necessary and reasonable for the Union to disclose the personal information to collect the debts owing to it. I will consider these factors separately, below.

Sensitivity

[39] In my view, financial information connected to an individual is generally sensitive information, particularly when it involves a debt. Owing money to another party (whether an individual or any legal entity) is generally a private matter between those parties. In my view, the fact that money was borrowed and is owed could, whether justified or not, lead to moral judgements about the individuals and their spending, financial choices, earning power or about their character generally. In particular, a lapse in, or lack of, payment to that party may be considered particularly sensitive information, given the stigma that may be attached to an individual having a delinquent debt.

[40] In this case, the Union points out that all members were aware that they were required to pay back the strike pay. However, there is no indication that before the list was distributed members knew how much strike pay their colleagues had received (including whether they had cashed the strike pay cheque they may have received) or how much any of them still owed. In my view, the financial information disclosed constitutes moderately sensitive personal information.

Amount of information disclosed

[41] The email disclosed the following information:

---

[26] Union submissions, paras. 12 and 13.
[27] Union submissions, para. 7.

- the individual's full name;
- the total amount of strike pay paid to the individual;
- whether the individual had not cashed or returned the cheque;
- how much the individual had repaid by December 5th;
- how much the individual had repaid by January 17th; and
- the total amount outstanding per individual.[28]

[42] The amount of information disclosed in this case was, in my view, more than what was necessary to collect the debt. Even if, as the Union contends, it was necessary to disclose some of the information about money owing, there is no evidence before me that establishes any reason to disclose whether the member had cashed their cheque or how much they owed as of particular dates.

[43] Therefore, in my view, the amount of information disclosed was both unreasonable and unnecessary in these circumstances.

Manner/scope of disclosure

[44] A reasonable person borrowing money would be aware that the organization was recording the information in order to manage the debt and that it may need to disclose the information to a select few, if their help was needed to collect the debt. However, one could not reasonably expect that the organization would have any cause to disclose the debtors' names and amounts owing to the entire union membership.

[45] As well, none of the debts were delinquent. However, even if they were, the Union had apparently not informed its members of the due date for repayment. Thus, the reason for disclosing the information when it did is not self-evident and the Union does not explain or provide any evidence as to why this was necessary or reasonable in the circumstances.

[46] Moreover, sending out the group email resulted in not only 12 individual Union members having access to all of this information, but also resulted in someone from the Union printing out the personal information and leaving it in the lunchroom for colleagues, management and other people to see. This was, in my view, not a reasonable manner or scope of disclosure in the circumstances and was not necessary to collect the debt.

Effectiveness

[47] In this case, the Union provided no evidence as to whether the disclosure was effective in collecting the debts. Therefore, I am unable to find that the disclosure was effective, or even assisted, in recovering any of the money owed.

[28] Complainant submissions, document 5.

Less privacy-intrusive alternatives

[48] While there is nothing that requires an organization to implement the least privacy-intrusive measure, it must balance its interests with the right of individuals to protect their personal information. As well, an organization must be prepared to demonstrate it gave reasonable consideration to any less privacy-intrusive measures.[29]

[49] There is no evidence in this case that the Union gave any consideration to other methods to collect the debt. In my view, this is unreasonable in the circumstances, given that the Union could have used several other means to achieve its purpose. For example, it had each individual member's contact information and could have sent out private emails or letters without disclosing any other member's personal information.[30] The Union could have also posted general notices about when the debt was due, or discussed it at a meeting and then sent follow up letters to individuals closer to the due date.

[50] In conclusion, I find that there were other less privacy-intrusive means to achieve the purpose of debt collection and that there is no evidence that the Union gave any consideration to these alternatives before disclosing the information.

Other factors – collective debt

[51] The Union appears to argue that because the members belong and contribute financially to the Union, they are all entitled to know how much each member owes the Union at any given time. I could not find any law supporting the proposition that personal information of this type should be accessible to every member of a union or organization, nor did the Union refer me to any.

[52] However, even if there was such a legal principle, the Union does not address the fact that this information was also disclosed to non-members, such as contractors, the employer and anyone else who may have had access to the unlocked lunchroom.

[53] Furthermore, I do not accept that using "moral suasion" is a reasonable or necessary first step to collect a debt. I would not go so far as to state that an organization can never prove the reasonableness or necessity of publicly disclosing information about individuals and their outstanding debts in order to collect that debt. However, in my view, it would take exceptional circumstances to meet this high threshold.

---

[29] Order P12-01, 2012 BCIPC 25 (CanLII), para. 145.

[30] It appears from the documents that the Union may have sent out some individual letters in December of 2014 regarding the debts but did not do this with all members. In any case, there is no evidence that the complainant received such a letter.

[54] There was no evidence in this case that any exceptional circumstances apply such that it would be reasonable or necessary to publicly disclose the personal information. Given all of the circumstances involved (*i.e.*, the sensitivity of the financial debt information, the failure to communicate a deadline for repayment prior to the disclosure, the exposure of the information to members and non-members, *etc.*), I find that the Union's decision to disclose the financial information in the manner it did, failed to appropriately balance the members' privacy rights with its own interests.

Conclusion, s. 18(1)(g)

[55] For the reasons noted above, I make the following findings:

- the information disclosed was moderately sensitive;
- the amount of information disclosed was unreasonable and unnecessary in the circumstances;
- the manner/scope of disclosure was unreasonable and unnecessary, and likely resulted in both members and non-members viewing the personal financial information;
- there is no evidence that the disclosure was effective in recovering the debts; and
- there were less privacy intrusive measures that could have been taken to collect the debt but it does not appear that the Union considered any of them before disclosing the information in the manner it did.

[56] Therefore, I find that it was neither reasonable nor necessary for the Union to disclose the personal information in order to collect the debts.

[57] A relatively recent case summary issued by the Office of the Privacy Commissioner of Canada supports my findings in this case.[31] PIPEDA Incident Summary #10 dealt with a case where an organization posted a list of its customers who had overdue accounts, as well as the corresponding amounts owed, onto a Facebook page. The organization submitted that s. 7(3)(b) of PIPEDA applied. Section 7(3)(b) is similar to section 18(1)(g) of PIPA in that it allows disclosure of personal information without consent in order to collect a debt. The Office of the Privacy Commissioner of Canada determined that the public posting was contrary to PIPEDA and the organization agreed to remove it.

[58] In the summary, the Office of the Privacy Commissioner of Canada stated:

> Our Office explained that, for example, this exemption to consent under PIPEDA allows for disclosing the debtor's personal information to a third-party debt collector who is acting as the agent of the organization owed.

[31] PIPEDA Incident Summary #10, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/incidents/2016/010_160125/.

> It does not, however, allow organizations to publicly disseminate information about their debtors without the debtors' knowledge or consent.

[59] In my view, this illustrates that the federal Office of the Privacy Commissioner views disclosing personal information in order to collect a debt in a narrow manner and does not support public "shaming" in order to collect a debt.

Section 34 – protection of personal information

[60] Section 34 requires an organization to make reasonable security arrangements to protect an individual's personal information. It states the following:

> 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

[61] To meet the reasonableness standard for security arrangements, organizations must ensure that they have appropriate physical, administrative and technical safeguards. Physical safeguards are tangible measures such as locking file cabinets, restricting employee access to storage areas and shredding papers. Administrative safeguards are measures such as regular privacy training, conducting privacy audits and ensuring that sensitive information is accessible only to those employees who need to know the information. Lastly, technical safeguards involve implementing measures such as using strong and secure passwords, encrypting personal information and using firewalls and antivirus software to protect personal information.[32]

[62] Whether security measures are reasonable is measured by whether they are "objectively diligent and prudent in all of the circumstances." Evidence of an individual's subjective opinion in that regard is, on its own, insufficient to establish this. While the reasonableness of security measures does not necessitate perfection, it may require a "very high level of rigour", depending on the circumstances.[33]

[63] The factors to consider when determining whether security arrangements are reasonable in the circumstances include:

- the sensitivity of the personal information;
- the foreseeability of a privacy breach and resulting harm;

---

[32] For further information on security arrangements, see the OIPC's *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*, published October 2015 (5th publication), online: https://www.oipc.bc.ca/guidance-documents/1438.

[33] Investigation Report F06-01: Sale of Provincial Government Computer Tapes Containing Personal Information, 2006 CanLII 13536 (BC IPC), para. 49.

- the generally accepted or common security practices in a particular sector or kind of activity;
- the medium and format of the record containing the personal information;
- the prospect of criminal activity or other intentional wrongdoing; and
- the cost of security measures.[34]

Parties' Positions

[64] The complainant submits that he is concerned about the Union's use of the school district's scanner and computer to disseminate the list containing the members' names and corresponding outstanding amount owing. However, his main concern appears to be that the list of names and amount owing was sitting on a table in a shared lunchroom and was "laying in plain sight for any passerby to view at their leisure."[35] He further notes that the lunchroom is not a locked space and it is available for use to other employees, not all of whom are union members.[36]

[65] The Union submits that the complainant "does not establish that the Union failed to make reasonable security arrangements…."[37] The Union also provided the OIPC with a copy of its Privacy Policy, which it says demonstrates that the Union has taken the following steps in order to protect its members' personal information:

> Access to personal information is limited to selected employees who require access to the information in the performance of their job function.
>
> The Union has installed reasonable security safeguards to prevent unauthorized access on its computer system.
>
> The Union will not collect or disclose personal information for purposes other than what has been listed in this policy.
>
> …

Analysis and conclusion, s. 34

[66] In this situation, the personal information was emailed to 12 Union members in their respective work locations. In the complainant's case, someone who had access to the email then printed it out, as well as the attachment containing the personal information, and left in an unlocked lunchroom accessible to other members, as well as other people who were not members (such as management and contractors).

---

[34] Order P15-01, 2015 BCIPC 20 (CanLII), para. 54, citing Order P06-04, 2006 CanLII 37938 (BC IPC) at para 80 referring to Investigation Report F06-01, 2006 CanLII 13536 (BC IPC).
[35] Complainant submissions, para. 8.
[36] Complainant submissions, para. 8.
[37] Union reply submissions, para. 9.

[67] I have considered the factors cited in Order P15-01 and, in my view, the relevant factors in these circumstances are that the personal information was moderately sensitive and, given the number of people who had access to the emails, a privacy breach and the resulting harm was reasonably foreseeable.

[68] Regarding the physical, administrative and technical safeguards, the Union has not provided any evidence of any safeguards it considered or took when it disclosed the personal information.

[69] There is no evidence that any physical safeguards were put in place to protect the personal information, as it was placed in a public location where multiple parties had access to the information to view, copy or further distribute.

[70] Administrative safeguards refer mainly to policies and training that an organization puts into place to ensure that personal privacy is protected. As noted above, the Union does have a privacy policy that states:

> Access to personal information is limited to selected employees who require access to the information in the performance of their job function.

[71] However, it does not appear that the Union considered and/or complied with this policy when it sent out the original email. When the Secretary-Treasurer disclosed the information to the 12 original individuals who received the email, she did note that the information was "confidential", for "CMAW members only" and that she was "not asking to have this posted on your bulletin board right now."[38] As far I can glean from the submissions and records, these statements were the only measures that the Union took to attempt to protect the personal information.

[72] In my view, these were clearly not adequate instructions in order to prevent the disclosure of the personal information, as it was subsequently printed and placed in a public location. In particular, the use of the words "right now" with regards to posting the information on the bulletin board infers that there would not be an issue with doing so in the future. As well, there is no mention of the legislated privacy obligations the Union is bound by, just a brief note that the information is "confidential". This lack of awareness of privacy rights and obligations (or failure to effectively communicate the safeguards that should be taken to protect the personal information) points to the need for appropriate training regarding privacy rights and disclosure of personal information.[39]

[73] As noted above, the complainant is also concerned with the potential lack of technical safeguards in place to protect the personal information. Neither party provided any evidence regarding any technical safeguards (or specific lack thereof), although the Union notes in its privacy policy that it has "installed

---

[38] Complainant submissions, document 1.

[39] For more information regarding an organization's obligations under PIPA, see the OIPC's *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*.

reasonable security safeguards". However, given my findings on the unreasonableness of the physical and administrative safeguards in place, I recommend that the Union review its use of technical safeguards to protect its members' personal information to ensure it is compliant with s. 34 of PIPA.

[74] In summary, I find that the Union did not make reasonable security arrangements to protect the members' personal information in these circumstances.

CONCLUSION

[75] For the reasons above, I have determined that the Union was not authorized by s. 18(1)(g) to disclose the personal information in the manner it did. I also find that it did not make reasonable security arrangements, as required by s. 34, to prevent unauthorized disclosure of the personal information.

[76] The Union submits that there is no need to make an order under s. 52(3) in these circumstances, as there is "no indication" that disclosure of the personal information is ongoing. The Union also states that the information was not particularly sensitive given that the debt owed was not a unique circumstance to the complainant and was shared by "dozens of other members".[40]

[77] For the reasons noted above, I am not persuaded that the information is not sensitive and that the disclosure of personal information is not ongoing. In particular, the Union stated in its response to the complaint that updated lists with strike pay amounts still outstanding would be "sent to each department/location on a regular basis until all debts have been collected."[41] Although it is not clear whether the Union intends to carry through on this in the future, in my view this reveals a lack of understanding of the Union's obligations under PIPA and suggest that a specific order prohibiting reoccurrence is needed here.

[78] There are previous orders where OIPC adjudicators have determined that there was no need to issue an order in the particular circumstances. For example, in Order P06-03, former Commissioner Loukidelis declined to issue an order due to the following circumstances: the disclosure occurred very shortly after PIPA came into force, it was not a serious breach, there was no indication that disclosure of the complainant's name was ongoing, the disclosure occurred approximately two years prior to the decision and the organization no longer owned the business in question.[42]

---

[40] Union submissions, para. 20.
[41] Complainant submissions, document 4.
[42] Order P06-03, 2006 CanLII 32981 (BC IPC), paras. 21 and 22.

[79] In my view, none of these mitigating circumstances are present in this case, and there is some indication that the Union does not fully understand its obligations under privacy legislation.

[80] For the reasons above, I make the following orders under s. 52(3) of PIPA:

1. The Union is required to stop disclosing personal information pursuant to s. 18(1)(g) in circumstances such as those described in this order; and

2. The Union is required to protect the personal information in its custody and/or control, pursuant to section 34 of PIPA.

[81] The organization must comply with this Order on or before **Monday, March 20, 2017.**

February 6, 2017

ORIGINAL SIGNED BY

Carol Whittome, Adjudicator

OIPC File No.: P15-61606