



OFFICE OF THE INFORMATION  
AND PRIVACY COMMISSIONER  
NEWFOUNDLAND AND LABRADOR

**Report P-2021-003**

**May 6, 2021**

**Labour Relations Board**

**Summary:**

A Complainant filed a privacy complaint under the *Access to Information and Protection of Privacy Act, 2015* (“*ATIPPA, 2015*” or “the Act”) with this Office regarding a privacy breach by the Labour Relations Board (the “Board”). The breach was the disclosure of personal information of a number of individuals who had signed union cards. The Labour Relations Board acknowledged the privacy breach. The Commissioner recommended that the Labour Relations Board review its policies and procedures for protecting and disclosing personal information; develop a policy and procedure for responding to privacy breaches; and to develop a remediation plan.

**Statutes Cited:**

[Access to Information and Protection of Privacy Act, 2015](#), SNL 2015, c. A-1.2, s. 64

[Labour Relations Act](#), RSNL 1990, c.L-1, sections 18 and 122

**Authorities Relied On:** [Protection of Privacy, Privacy Breach Protocol March 2015](#)

## I BACKGROUND

- [1] A Complainant, on behalf of another individual who provided consent, filed a privacy complaint with this Office under the *Access to Information and Protection of Privacy Act, 2015* (“*ATIPPA, 2015*” or the “*Act*”) regarding a breach of privacy. The Labour Relations Board (the “Board”) disclosed signed union membership cards to an employer.
- [2] The Board advised that on August 13, 2020 it received an Application for Certification (the “Application”) from the Complainant via e-mail. The Complainant was advised to re-file as there was an issue with the Application and the legibility of the membership cards. Later that same afternoon, the final Application was received via e-mail. The Application and membership cards were sent together in a single PDF document.
- [3] On August 14, 2020, the Board instructed an employee to process the Application. In the normal course of processing an Application for Certification, the Board would provide an employer with notice of the application, a copy of the application for certification, and applicable legislation. Union membership cards are not provided to the employer. In the within matter, the Board employee prepared an e-mail to the Employer attaching the PDF document received from the Complainant. By doing so, the Board employee included 37 confidential union membership cards.
- [4] Following the inadvertent disclosure of the membership cards to the Employer, 23 of the employees who had applied to certify the union were laid-off by the Employer. The Complainant believes that this action was taken as retaliation against the employees’ efforts to certify the union and such retaliation was only possible because the Board had disclosed personal information to the Employer.
- [5] The Board explained that, prior to March 17, 2020, Applications had to be accompanied by original membership cards to show support for the Application. The original membership cards would have been provided to the Board in person or by mail.

- [6] To reduce the risk of spread of COVID-19 and to conform to government policies, one of the measures taken by the Board, effective March 17, 2020, was to only accept filings electronically, including Applications.
- [7] Prior to sending the Application, the Board employee did not realize that the union membership cards were attached to the Application before it was forwarded to the Employer's representative. The Board advised that union membership cards are not typically attached to Applications.
- [8] Upon discovering the error, the Board contacted the Employer, and a representative of the Employer advised he had not opened the PDF containing the Application. However, the Employer's representative subsequently advised that the e-mail had been forwarded to his supervisor and the PDF containing the membership information had been opened.
- [9] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 74(2) of *ATIPPA, 2015*.

## II PUBLIC BODY'S POSITION

- [10] The Board acknowledged that the disclosure of the membership cards was a breach of privacy.
- [11] The Board advised that the breach was discovered very shortly after the e-mail was sent to the Employer and the Board attempted to recall the e-mail immediately upon discovery of the breach, however the recall was unsuccessful.
- [12] The Board then proceeded to contact the Employer's representative. All communication regarding the privacy breach with the Employer's representative was done by telephone. The Board asked the Employer's representative to delete the e-mail from his inbox and his deleted mail folder. The Employer's representative was advised that the e-mail was sent in error. The Employer's representative advised that he had only just opened the e-mail, because he was in meetings all morning. He advised that he had only opened the PDF containing the covering

letter and had not yet opened the PDF containing the Application, which also contained the membership cards.

[13] The Board indicated that the Employer's representative questioned if he was sent something he was not supposed to see, and the Board responded that confidential information that the Employer should not be privy to was accidentally forwarded to him. He again advised the Board that he did not read the attachment. The Board indicated that it did not want to advise the Employer's representative of the exact content of the information for fear that he may not actually delete it.

[14] A corrected e-mail was sent to the Employer's representative, attaching the Application without the membership cards.

[15] That same afternoon, the Board's ATIPP Coordinator contacted the Complainant's counsel by phone to report that there was a privacy breach on the Board's part when membership information was included in the Application sent to the Employer. Counsel was informed that an attempt was made to recall the message and that the Employer advised that it had not read the attachment.

[16] The ATIPP Coordinator informed the Complainant that it was the first time anything like that had happened at the Board and apologized for it.

[17] On August 18, 2020, the Employer's representative informed the Board's CEO that the e-mail had been forwarded to his supervisor and the PDF containing the membership information had been opened.

[18] The Board indicated that it followed the information provided on this Office's website and the procedures set out in the Privacy Breach Protocol (March 2015) which included containing the breach, evaluation of the risks, notification of affected individuals and prevention of future breaches.

[19] The Board already explained above how it attempted to contain the breach. Regarding the evaluation of risk, the Board stated:

*The information that was provided is extremely sensitive and has the potential for repercussions for the affected individuals associated with the breach of privacy. If an employer views membership cards, the individuals noted could face potential reprisal from that employer for participating in an organizing drive. This could potentially result in job loss for the affected individuals. This risk is present as long as the affected individuals remain employed with that employer. The Employer's representative acknowledged that he forwarded a copy of the initial e-mail to his supervisor and that his supervisor reviewed the confidential information. As a result, there is the possibility that other individuals could gain knowledge of that confidential information through dissemination by the supervisor. Individuals are protected against job loss as a result of participating in a trade union pursuant to Section 24 of the Labour Relations Act. Individuals are also protected against changes to the terms and conditions of employment pursuant to Section 45 of the Act, this reduces the risk for potential harm to individuals.*

*Risks associated with the personal information (date of births, addresses, SINs, etc.) contained on the membership cards should be minimal as the Employer would have already had that information. There is a risk of harm to the Board and the general public in that there could be a loss of trust in the integrity of the Board's processes and a "chilling effect" on employees who are considering whether to sign union membership cards.*

[20] The Board reported the privacy breach to this Office on August 17, 2020 in accordance with section 64(4). The Board sent notification letters to the individuals affected. Initially, the individuals were contacted by phone and then provided with a formal letter notifying them of the breach. However, it was only after this initial notification that the Employer's representative advised that the e-mail had been forwarded to his supervisor and the membership information opened. The Board then re-notified the individuals with this additional information.

[21] In an attempt to prevent further breaches of this nature, the Board revised its practice of accepting electronic membership cards and information. The Board issued a notice on September 1, 2020 advising the labour relations community that it would no longer be accepting electronic membership cards and that it would only be accepting cards in person or by mail. The Board advised that cards would now be verified in the presence of a union

representative and copies will be sealed in an envelope and kept in a locked cabinet. If the Board finds it necessary to review the cards at any time, the union will first be notified in advance and be provided an opportunity to attend while the Board reviews the cards. If a union's representatives are unable to attend, two Board Officers will be present to review the cards and re-seal them as necessary. Upon the conclusion of a file, the sealed membership information will be destroyed.

[22] The Board indicated in this notice that it would be conducting a full review of its policies, practices and procedures covering union membership information. The Board also advised it planned to develop an appropriate remediation plan.

[23] The Board explained that there has been significant turnover of staff in recent years. The Board stated that the excessive periods of staff shortages have resulted in job sharing of the duties and responsibilities of the vacant positions and excessive workloads for the staff, and that given the nature of the Board's work, this excessive workload has increased the potential for errors. As part of the review of its policies, procedures and practices the Board stated it will be seeking to address its staffing needs.

[24] The Board accepts full accountability for the breach of confidential information and has apologized for its actions.

### III COMPLAINANT'S POSITION

[25] The Complainant states that membership cards, which provide evidence of membership, are supposed to be treated with the highest level of respect and sensitivity and are never supposed to be disclosed to an employer or any third party.

[26] The Complainant indicated that confidentiality is necessary because an employer who is aware an employee has signed a union membership card can discriminate against the employee on the basis of union membership, or target the employee for retribution.

[27] The Complainant has acknowledged that the Board had admitted its error in releasing the membership evidence and has put in place additional procedures to prevent a future occurrence. However, the Complainant does not believe that the Board took adequate steps to ensure that the Employer had actually destroyed the electronic information and also that it had not used it against the union and its own employees.

[28] The Complainant stated that the Board did not use its statutory investigatory powers to compel the Employer to provide further information on its dissemination and use of the confidential membership cards and that the Board has failed to act. The Complainant submits that the Board has powers under section 18 of the *Labour Relations Act* to compel a party to provide information or produce documents and that this authority could have been exercised to obtain greater confirmation that the e-mail had been properly deleted. The Complainant felt that the Board was content to accept the word of the Employer and that while the informal manner in which the Board directed information requests to Employer may have followed its usual practice, in this case the practice followed was both ineffective and inappropriate as it related to obtaining information about the access and use of confidential information.

[29] The Complainant further submits that the Board did not and has not demanded copies of all e-mail or letter correspondence relating to the internal or external distribution of the information contained in the membership cards.

[30] It is the Complainant's opinion that the Board's conduct and its lack of an adequate response to the privacy breach has become an issue of critical importance to the trade union movement and its members throughout Newfoundland and Labrador. The Complainant believes that it was incumbent on the Board to use its powers to ensure the information disclosed in the privacy breach was not misused by the Employer.

[31] Finally, the Complainant states that the Employer laid off those employees who signed the membership cards and the Complainant further alleges that the Employer acknowledged to laid-off employees that their termination was connected to them signing the union membership cards and the Employer having access to same.

#### IV DECISION

- [32] The information on the membership cards is clearly personal information as it consisted of names, addresses, phone numbers, dates of birth, social insurance numbers, and signatures. The intent to affiliate with the Union is also personal information, as defined in section 2(u)(ii) and 2(u)(ix) of *ATIPPA, 2015*. The membership cards indicate the employee's intent to affiliate with the Union and this would be the individual's political beliefs or associations as well as the individual's personal views or opinions. The employee's personal information, including their intent to affiliate with the Union, was disclosed by the Board to the employer in contravention of section 64(1)(a) of *ATIPPA, 2015*.
- [33] While the Board has acknowledged and responded quickly to the breach, the main concern from the Complainant is how the Board attempted to confirm that the e-mail with the membership cards was not opened or read and had been deleted.
- [34] Public bodies in the past have accepted verbal confirmations that personal information sent in error was deleted and not forwarded on. This method puts a lot of trust in the individual the public body is dealing with to be truthful, and it is more appropriate to circumstances where the information is less sensitive and the recipient has no personal or professional interest in the content of the information. Due to the sensitivity of the information on the membership cards, the fact an Application was submitted to the Board, and that the membership cards were now accessible to the Employer – a party with interests opposed to those of the membership applicants – the Board could have requested more evidence that the e-mail was in fact deleted and not forwarded to other individuals.
- [35] In following the ATIPP Office's Privacy Breach Protocol (March 2015), the Board did follow the steps for containing the breach. The Board attempted to recall the e-mail, and it then contacted the Employer's representative requesting the e-mail be deleted, and then a supervisor was contacted and informed of the breach and the breach was reported to this Office. While these steps were followed, the weak link appears to be the communication with the Employer's representative that frustrated the Board's attempts to contain its breach.



[36] The Board could have requested a written confirmation that the e-mail was deleted along with all attachments and that it was not forwarded on. The Board could have even requested an affidavit if they felt that was necessary. The acceptance of the verbal confirmation from the Employer's representative did not end up being robust enough in this case to fully contain the breach.

[37] In evaluating the risks, the Board did note to our Office that sections of the *Labour Relations Act* (in particular, sections 24 and 45) protect individuals against job loss and changes in the terms and conditions of employment, so the Board did turn its mind to this possibility. The Board can initiate an investigation upon a complaint under the *Labour Relations Act*.

[38] The Union filed a complaint with the Board pursuant to sections 18 and 122 of the *Labour Relations Act* against the Employer alleging that management employees of the Employer accessed and used the membership cards in their decision to lay-off employees and also threatened, harassed and intimidated the employees. The Union alleged that the Employer contravened subsections 23(1)(a), 24(1)(a), 25(1) and 25(3) of the *Labour Relations Act* and sought a determination that there had been unfair labour practices by the Employer pursuant to these sections. In relation to the employees that were laid off, the Union requested that the Board order the reinstatement of discharged employees with full compensation for all lost wages and benefits. The outcome of this complaint is that the Union reached an agreement with the Employer and the Employer is voluntarily joining the Union. The Union advised that the action with the Board is now over as the parties have reached an agreement.

[39] In an attempt to prevent future breaches, the Board changed its use of e-mail for accepting Applications and issued a notice on September 1, 2020 to the labour relations community advising that it would only be accepting membership information in physical paper format, and once reviewed it will be sealed by the Board in the presence of a union official, subject to any COVID-19 protocols.

[40] The Board noted that it planned to develop an appropriate remediation plan to address privacy breaches in general but also to specifically focus on the protection of membership

cards from disclosure. The Board also plans to conduct a full review of its policies and procedures.

[41] Often complainants, and perhaps members of the general public, are under the impression that the OIPC can impose penalties or award damages in situations where a privacy breach has, or has alleged to have, harmed individuals. This is not the role of the OIPC under *ATIPPA, 2015*. While there is an ability for the Commissioner to lay charges against individuals, subject to prosecution by the Crown, this is limited to intentional breaches. There is no public sector privacy statute in Canada that provides a privacy commissioner with the authority to levy penalties against public bodies regarding a breach that is not intentional, as was the case here. Our role is instead to make recommendations, as we have done here, on the adequacy of a public body's policies and procedures. The *Privacy Act* does contain a private right of action considering a violation of privacy as a tort, but individuals must bring that right of action to court directly themselves under that Act and the OIPC has no role. In this particular instance, as noted, the Labour Relations Board itself has remedial authorities vis-a-vis the actions the Employer may have taken following that breach; however, as further noted, it appears that the Employer and the Union have come to an agreement on the matter.

## V RECOMMENDATIONS

[42] Under authority of 76(2) of *ATIPPA, 2015*, I recommend that the Board:

1. Review its policies and procedures regarding disclosure of personal information, specifically with regard to membership information;
2. Develop a policy and procedure for addressing privacy breaches, including steps for containing the breach;
3. Develop an appropriate remediation plan for privacy breaches;

[43] As set out in section 78 of *ATIPPA, 2015*, the head of the Labour Relations Board must give written notice of his or her decision with respect to these recommendations to the

Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[44] Dated at St. John's, in the Province of Newfoundland and Labrador, this 6<sup>th</sup> day of May 2021.



Michael Harvey  
Information and Privacy Commissioner  
Newfoundland and Labrador