

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

**Report on an Investigation into Reasonable Safeguards and
Retention of Personal Information in Custody of a Union**

September 14, 2006

Alberta Regional Council of Carpenters

Investigation P2006-IR-004

I. INTRODUCTION

[1] On May 20, 2005 this Office received a complaint in respect to the Alberta Regional Council of Carpenters Union's ("RCC") activities under the *Personal Information Protection Act* ("PIPA" or "the Act"). The Complainant was concerned that the RCC:

- did not properly assist him when he sought information on security measures employed by the International Union;
- did not have reasonable safeguards to protect membership information in the local and international environment; and
- was retaining membership information beyond what was necessary for its business purposes.

II. JURISDICTION

[2] The Act applies to provincially-regulated organizations in Alberta. The Commissioner has jurisdiction in this case because the RCC is an "organization" as defined under subsection 1(i) of the Act.

[3] On June 7, 2005, the Commissioner authorized me to conduct an investigation under subsection 36(2)(e) of the Act and to attempt to bring the matter to a successful conclusion.

III. INVESTIGATION

[4] The Complainant is a union member based in Edmonton, Alberta. The United Brotherhood of Carpenters and Joiners of America is an

international union representing carpenters and allied trades (“International Union” or “International”). The RCC is a chartered council of the Carpenters International Union and is the central governing and policy-making body for all locals in Alberta and the Northwest Territories. Locals 1325, 2103, 2010 and 1460 are members of the RCC.

[5] In conducting this investigation, I spoke with the Complainant and with counsel for the RCC and received their submissions, met with the Canadian Director of Research and Special Programs and the Vice President of the Canadian District, United Brotherhood of Carpenters and Joiners of America, and the Executive Secretary Treasurer of the RCC. I also discussed the matter with the Privacy Officer for the RCC. In addition, I examined privacy policies and security practices for the local and international union, union constitution documents, employment standards and agreements, and related forms and descriptions of procedures. I also reviewed court documents related to a dispute between the RCC and others, and a former employee and other unknown persons (July – December 2005).

IV. STATEMENT OF FACTS

[6] The International Union maintains personal information about their members in an electronic system called “ULTRA”. This system is a member record-keeping system that is capable of recording information about each union member, including their name, address, phone number, birth date, language, citizenship, gender, employer, membership status, classification, political affiliation¹, age and years of service. The electronic system was developed in 1998 using proprietary software owned and developed by the International Union. The system was developed to improve access to and control of member records. The servers are located at the International Union’s data centre in Las Vegas, Nevada.

[7] The Complainant specifically stated that in May of 2005, he requested information on the “ULTRA System” because he was concerned about the security of members’ data. He inquired:

“how it works with the use of my SIN number and how the International Union is using SIN numbers”.

[8] He alleged that he made a verbal request for this information to the

¹ The RCC does not actually collect this information as this information is not reasonably required by the Organization.

RCC's Privacy Officer. He stated that he later received a verbal response from the Privacy Officer that his request was denied by the Executive Secretary Treasurer and was instructed to communicate directly with the International Union. She had been designated in that role but no training had been provided; her decision-making authority was unclear to her at the time of the Complainant's inquiry.

[9] The Complainant then contacted our Office to file a complaint about the RCC. He was concerned about the union's failure to respond to his inquiry about the ULTRA system, and had concerns about the security and confidentiality of union members' personal information at the local and international level. The Complainant was also concerned about the retention of member information in electronic and paper based systems.

[10] I was informed by counsel for the RCC that each International Union affiliate is required to use the system for their dues processing and membership record keeping by accessing servers at the International data centre. Transactions are entered at the affiliate or local level but the software and data exist only at the International Office. In essence, the local unions are remotely entering data into a mainframe server through the internet. Local access to the ULTRA system is administered and controlled by each Regional Council. In Alberta, the RCC's Executive Secretary Treasurer authorizes various levels of access depending on a person's position and level of responsibility.

[11] In July 2005, during the investigation of this complaint, an incident occurred involving an alleged breach of privacy and confidentiality of membership information by a dispatcher for Local 1325 and 2103. The RCC alleged that the Dispatcher exported membership information from the ULTRA database and from an internal database operated locally through the Edmonton union. The RCC alleged that this individual accessed the systems from his own home computer and, in response, it sought redress through the courts. The Complainant brought the incident to my attention as evidence of lax security measures by the union.

[12] The Dispatcher was located in Edmonton and his primary duties involved receiving requests for workers from employers and dispatching to those jobs members who were not working. He was also responsible for maintaining the website operated by the RCC in Edmonton, the office computer system and other computer related duties. His duties required him to access the ULTRA system. He was also responsible for the development, maintenance and use of an Access Dispatch Database in the Edmonton offices of the RCC. The database contained personal membership information including name, address, phone number, SIN,

skills and bidding history of all the members of the locals. In the court documents, the RCC and its expert witness presented evidence that active steps had been taken to undermine the security of the computer system and all data on it. In his affidavit, the Dispatcher confirmed that he had installed and configured a file sharing program which circumvented the security of the systems and permitted a software download.² The Organization alleged that this activated remote access to the employee's computer so that he could copy all confidential information, including accessing the ULTRA system and the Access Dispatch Database from home or other locations.

[13] The RCC and the other unions involved in the dispute were successful in obtaining an interim injunction against the Dispatcher. Although the *extent* of the removal of information from the Organization's computer system has not been absolutely proven, the court order restrains the Dispatcher and any other persons from retaining or making use of the Unions' confidential membership information.³

V. ISSUES

[14] To resolve this matter, I must determine the following:

1. Did the RCC fulfill its obligation to assist the Complainant who was requesting information regarding the use of Social Insurance Numbers ["SINs"] in the ULTRA system?
2. Did the RCC have reasonable safeguards at the local and international level?
3. Did the RCC retain personal information in excess of its business purposes?

1. Analysis of Duty to Assist

[15] Under section 27 of the Act:

(1) an organization must

a. make every reasonable effort

*i. to assist **applicants**, and*

ii. to respond to each applicant as accurately and completely as reasonably possible.

[16] It is uncontested by the Organization that the Complainant requested information about the use of SINs in the ULTRA system and at the international level. This inquiry was a verbal request to the RCC's

² Action No. 0503 14334, Court of Queen's Bench of Alberta, Edmonton, Judicial District of Edmonton, cross examination on affidavit, August 23 and August 29, 2005, pg 174—184).

³ Action No. 0503 14334, Court of Queen's Bench of Alberta, Edmonton.

Privacy Officer; it was not made in written form. Therefore the Complainant is not an “applicant” as defined in section 23(a) of the Act that states:

“applicant” means an individual who makes a written request in accordance with section 26’.

[17] However, I believe that the Privacy Officer and/or senior officials had a duty to suggest that the individual put his request in writing, thus triggering the right of access under section 24(1)(b) which allows the individual access to:

“The purposes for which the personal information ... has been and is being used by the organization”.

[18] The RCC’s access and privacy policy only addresses responses to written requests from individuals; therefore, I find that there was a positive duty to inform him that his request had to be in writing in order to get a response, rather than referring him to the International Union.

[19] Moreover, under section 6 of PIPA, organizations must:

*(a) develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act, and
(b) make information about the policies and practices referred to in clause (a) available on request.*

[20] The International Union issued a policy statement regarding the use of SINS in February 2003. They implemented an internal ID number to replace the use of the Social Security⁴ and SINS as a member’s file or identification number, restricted the use of these numbers, and implemented further controls for printed documents containing SINS.

[21] I believe it would have been relatively easy for the RCC Privacy Officer or the Executive Secretary Treasurer to provide a copy of this policy to the Complainant, rather than referring him to the International Union. It may have eased some of his concerns about the security of the data. I find that RCC contravened section 6(b) of PIPA in failing to respond to the Complainant’s request for policy information.

[22] However, I cannot find that Organization contravened section 27 in failing to advise the Complainant of his right to file a written request for access under the Act because the complainant is not technically “an applicant” as defined by the Act.

⁴ The Social Security numbers in the US are equivalent to SINS in Canada.

[23] Since this incident, the RCC has implemented a policy that details the responsibilities of the Privacy Officer, including annual reporting requirements, proactive policy dissemination and a complaint-handling process. In the spirit of the “duty to assist” the RCC has agreed to enhance this policy by including a process for responding to informal requests for access to information.

2. Analysis of Adequacy of Safeguards at the International and Local Levels

[24] Section 34 of the Act states:

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.

[25] Section 2 of the Act defines the “reasonableness standard” as follows:

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.

[26] In Investigation Report F06-01, Information and Privacy Commissioner for British Columbia David Loukidelis considered what the reasonableness standard means in the context of the public sector law in that Province.

“by imposing a reasonableness standard in s. 30 [equivalent to section 34 of PIPA], the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one’s personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, “reasonable” does not mean perfect. Depending on

the situation, however, what is “reasonable” may signify a very high level of rigour.”

[27] Standards or technologies prescribed in legislation would be quickly outdated. Rather, the reasonableness standard acknowledges that the sensitivity of the data, the level of risk or threat of unauthorized access or disclosure and the measures applied to protect the data will vary and may change over time.

[28] I believe that it is incorrect to assume that an employee’s unauthorized use and disclosure of personal information is conclusive evidence of unreasonable security practices. Although under PIPA, organizations are responsible for the actions of their employees⁵, intentional wrongdoings by a trusted employee who legitimately required full access to the system for his job functions is not conclusive of a breach of section 34. However, PIPA requires that organizations take measures to guard against reasonably foreseeable risks.

[29] I find that the *extent* of the unauthorized use and disclosure of members’ information from the ULTRA system and the Access dispatch database was **not** a reasonably foreseeable risk. The employee in question had worked for the RCC for over six years and was also an elected officer of Local 1325. He had been given increasingly responsible tasks and his supervisor did not have evidence of any problem. The RCC argues that this employee was responsible for taking steps to set up a secure website, a secure dispatch procedure and secure computer systems for the Organization. Court records⁶ indicate computer forensic experts determined that a file-sharing program which allowed persons to bypass the security of the computer systems, download unauthorized software and activate remote access to the work computer was activated. I do not believe that these actions could have been reasonably foreseen by the Organization.

[30] The RCC acknowledges that there is motivation for members’ information to be disclosed to third parties for unauthorized purposes due to the competitiveness within the building trades union environment (the potential for raiding between rival unions). Membership information also has commercial value in today’s tight labour market because non-union employers may wish to attract individuals to their employ. Because of these risks, the international and local union historically included express confidentiality standards in its international constitution and its local by-laws. Confidentiality and privacy provisions

⁵ An analysis of vicarious liability is outside the scope of this investigation.

⁶ Action No. 0503 14334, Court of Queen’s Bench of Alberta, Edmonton

are also included in contracts of employment which pre-date PIPA. The extent of confidentiality and security measures pre-dating legal requirements demonstrate that the Organization foresaw a risk of unauthorized access to the data, but not the by-passing of all security and downloading of data by a trusted employee who had authorized access.

[31] The most likely risk identified by the RCC involved unauthorized use and disclosure of members' contact information, rather than more sensitive personal information that could be used to harm the financial, work or personal lives of affected individuals. Since the most likely unauthorized use of personal membership data was for the purpose of contacting members (arguably more harmful to the RCC and its union locals than to the individual member), the RCC did not apply more stringent safeguards.

What preventative measures were in place?

[32] At the time of this incident and when the complaint was received, the RCC and the International Union had a framework of administrative and technical security and privacy measures⁷ in place to protect data in the ULTRA system and govern the use of that data by staff and union officials.

[33] I have reviewed these policies and received undertakings about the security features of the system. The policies include the training and dissemination of information about the system to all users. Users receive periodic reminders sent as "post it" notes posted on the system. They receive a quarterly newsletter which contains information on new procedures and issues of privacy, security and confidentiality. The International's Regional Councils are required to provide ULTRA users with training and technical support through their designated Key Users. Key Users are sent to the International Training Centre in Las Vegas for training; they are also required by the International's policy to monitor the activities of all ULTRA users and provide regular reports to expose any abnormal activity on the part of a specific user.

[34] The International's servers and data are housed in a locked, secured data centre which opened in 2001 in Las Vegas. Since 2001, the International Union has created five layers of security and privacy protection of all data it houses. The devices provide firewalls, virus protection, spyware protection as well as defenses against denial of service attacks, and other intrusions. The Organization advises that the Data Centre has never been breached nor penetrated by an unauthorized

⁷ Based on the investigator's review of policies, procedures and submissions by RCC.

individual or organization.

[35] All membership data is encrypted during transmission. The International uses 128 bit encryption between the server and the user. This level of encryption is equivalent to the system used by the banking industry. Access to the system requires an account name, password, and additional number challenge which changes with each log-in. The number challenge prevents automated attempts to guess at account names and passwords. Only the computer server knows an individual's password. Every user must change their password every three months.

[36] Auditing of the system is facilitated through the International and not the Local or Regional Office. The International Union uses custom programming to do more detailed auditing and look for any unusual patterns of activity. Additionally, at the request of a Regional Council, the International Union can turn on a key stroke auditing device that records every keystroke an individual makes. This is used only when an Executive Secretary Treasurer believes that additional scrutiny is necessary. In this case, the International union was able to identify unusual activity (a download of software) which triggered the investigation and termination of the Dispatcher.

[37] Every user on ULTRA has his or her own user account. By policy, no two users are allowed to share their accounts or passwords. Every user's action may be audited with every menu, screen and transaction recorded by user, date and time. Users are made aware of the auditing capacity of the system. Unauthorized use or access to ULTRA is grounds for immediate termination of an ULTRA account and the termination of the individual's employment with the International Union or affiliate.

[38] As mentioned earlier in this report, the International Union's SIN Policy provides for specific security and confidentiality safeguards. Access to this number is restricted on a need-to-know basis (it is available to only a limited number of users and there is no requirement that union locals be given access to the SIN). The policy restricts access and use of the SIN for income tax purposes, employer billing statements, and for security clearance at nuclear power plants and airports, where there is an enhanced need for verification of identity. No printed copies may contain the SIN except where the member needs security clearance at one of these sites.

What security measures were in place at the local (RCC) level?

[39] Although the International Union sets the policy and procedural framework for the ULTRA system, the security of the system is obviously vulnerable to its implementation at the local or regional level. To this

end, the following preventative measures were in place at the local level at the time of the complaint:

- Job descriptions with reviews and reporting structures in place for all positions.
- ULTRA system users received training in Las Vegas and receive ongoing reminders of policies and procedures.
- Contracts of employment containing confidentiality provisions, including a prohibition for disclosure of information to any party outside the organization and a termination for breach of any provision of the contract.
- Union constitution confidentiality obligation to read and sign upon application for membership.
- RCC protection of personal information which encompasses collection, use, disclosure, storage and safeguarding of personal information through policy and procedure.
- RCC By-Laws which address council's power to hire, discipline or terminate staff, and outline supervisory duties of council and Executive Secretary Treasurer.

[40] In reviewing these documents and the signed oath of the employee in this incident, I am certain that he would have been aware of the obligation to maintain confidentiality and privacy of the members' information.

[41] I find that the RCC had reasonable administrative and technical safeguards in place to protect the privacy of members' personal information and acted within the scope of its knowledge and abilities. I find that they had good measures in place to address the types of external and internal threats that were reasonably foreseeable. The extent and method of this breach could not have been reasonably foreseeable for the following reasons:

- Employee was a trusted senior staff member with no performance issues over 6 years
- Employee had been an elected official of the union
- Extensive security and confidentiality training provided to the employee
- Employee had taken confidentiality oath
- Log on procedures, audit capacity of system

[42] I hesitate to recommend that, in this case, more should have been done to protect against this type of threat by a trusted member of the staff who had legitimate access to the system. I considered whether every organization holding personal information in a computer system could

reasonably be expected to proactively monitor all employee activity with respect to every database. Such monitoring could include installation of surveillance cameras at every desk, keystroke logging software and audit capacity activated and monitored 24-7, and review of all internet activity and email. The International union had all of these tools available to them and implemented their use immediately upon suspicion of unusual activity. I find this to be a reasonable response. Implementing all of these measures for all employees has significant privacy and resource implications. I believe that expecting these measures in every case would be too onerous. I find that there was no reason for putting this individual under surveillance until unusual activity was detected by the system administrators. They acted reasonably in trusting him to abide by policies.

What post incident measure was in place?

[43] The RCC took the following steps to secure the data and to mitigate the risk of similar occurrences in the future:

- Within six days of the alleged export of the membership records, RCC's Executive Secretary Treasurer was advised by the International's Director of Technology of the problem.
- RCC then brought in an external information technology contractor to review the incident. The following day, the employee was terminated.
- Immediately after termination (the same day) RCC reviewed the employee's email, removed his pass code and blocked him from administrative access to the web site and access to the telephone system.
- Retained Deloitte & Touche to conduct a forensic investigation.
- Commenced legal action to protect the confidentiality of the exported data.
- Revised privacy policy to include detailed responsibilities for Privacy Officer and incident response protocol; added specific rules regarding remote access, laptop and electronic storage devices, and removal of records from the office.
- Outsourced Information Technology (IT) functions – taken steps to separate the functions of dispatcher and IT.

[44] I believe that RCC's actions were diligent and demonstrated best efforts in these circumstances.

3. Analysis of Retention Requirements – Section 35

[45] The Complainant was also concerned about the length of time

members' personal information was retained in the international and local system.

[46] Section 35 of the Act states:

Notwithstanding that a consent has been withdrawn or varied under section 9, an organization may for legal or business purposes retain person information as long as is reasonable.

[47] Member data in the ULTRA system and in the hands of RCC is currently retained in perpetuity.

[48] The RCC argues that there are sufficient reasons for this practice:

- Verification of union service for pension applications.
- Investigations of past union elections (eligibility to hold office at a particular time).
- Capacity of members to leave and then rejoin at later time – there may be a 10-year gap in returning to the union. Former members have different entitlements and levels of skill classification which may affect wage scale.
- Environmental health authorities may need to locate members who worked at various sites perhaps 40 or 50 years in the past.

[49] The only question to consider here is whether or not the business purposes for retention of the data are reasonable. Unlike British Columbia's PIPA, Alberta's PIPA does not contain a general obligation that an organization destroy documents containing personal information, or remove identifiers as soon as it is reasonable to assume that the information is no longer necessary for business purposes. PIPA only contains this obligation in regard to business transactions in section 22. PIPA also does not require an organization to establish minimum and maximum retention periods. However, I believe that for privacy best practices and data security purposes, organizations are well served by deleting or disposing of personal data no longer required for the purpose for which it was collected.

[50] There is a significant amount of detail in the ULTRA system. It includes (among other things) birth date, language, citizenship, gender, employer, membership status, classification, political affiliation, etc. Fifty or sixty years after withdrawing from the union, it is unlikely that that individual will be re-instated and require access to this information. There is also a likely maximum date for confirmation of pension requirements and administration of survivor benefits. Information will

lose its business value on the death of a member. As well, detailed information such as Social Insurance Numbers are unlikely to be needed for historical purposes. There are very few records (in a business setting) that require permanent retention.

[51] Once the organization has carefully considered the nature and extent of the personal information involved, and any specific legal requirements (such as any statutory limitation for civil lawsuits or under Health and Safety legislation), I believe the RCC can establish that only a core amount of data is needed for legal and business requirements. Any data fields that are not needed for long term business purposes could be purged at a specific trigger point (“X” years from membership enrolment date or at death).

VI. CONCLUSION

[52] I find that the RCC contravened section 6(b) of PIPA by failing to respond to the Complainant’s request for (existing) policy information regarding the use of SINS.

[53] I find that RCC implemented reasonable administrative and technical safeguards to protect membership information at both the international and local levels. The RCC may have foreseen the risk of unauthorized access to the system by an employee; however, executives could not have reasonably foreseen the extent and method of a data breach by a long-term employee who had legitimate access to the data to perform his duties. The safeguards in place at the time of the incident were adequate protection for internal and external risks that were foreseeable, but not for these exceptional circumstances. In recognition of the seriousness of this incident, the Organization enhanced and refined the safeguards already in place.

[54] RCC’s policies, procedures, technical security and response to this incident comply with the obligations in section 34 of PIPA.

[55] PIPA does not require organizations to destroy personal information once it is no longer necessary for business purposes. This is a best practice only. Therefore, the RCC is in compliance with Section 35 of PIPA.

VII. RECOMMENDATIONS

[56] I recommend that the union consider the retention of the data on a field-by-field basis, and investigate purging specific data in the ULTRA system on the death of each member.

[57] I recommend that the Organization use this incident to remind employees of the confidentiality and security requirements in the use of this system.

[58] Throughout this investigation, the Organization has taken steps to enhance and revise policies and procedures and communicate these policies with its employees. Therefore, I have no further recommendations in this regard.

[59] This file is now closed.

Elizabeth Denham, Director
Personal Information Protection Act