

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

**Report on the Investigation into Collection, Use and Disclosure of
Customer Information**

July 26, 2004

EPCOR

Investigation Report P2004-IR-001

I. INTRODUCTION

[1] In January and February of 2004, a number of individuals contacted the Office of the Information and Privacy Commissioner (OIPC) to report that EPCOR, an electric utility company (the “organization”), collected and used their personal information contrary to the *Personal Information Protection Act* (PIPA or “the Act”). The complainants were concerned about the amount and type of personal information collected for the purposes of identifying customers over the telephone, conducting credit checks and managing accounts (for example, when customers called in to change a service, change demographic information or provide a meter reading). The complainants stated that it was unreasonable to be required to disclose sensitive personal information such as Social Insurance Numbers (SIN), Alberta drivers license numbers, passport numbers, etc. for the purposes of managing accounts. They were most concerned about the collection, use and retention of their SIN as a form of identification and as a requirement for credit checks. There were a number of other callers during this time period with similar complaints; however, once the OIPC had already received four written complaints about this issue and this organization, subsequent complaints were not recorded.

II. JURISDICTION

[2] Except as provided in the Act and subject to the regulations made under it, as of January 1, 2004, the PIPA applies to all organizations in respect of all personal information. The Commissioner has jurisdiction in this case because an electric utilities company is an organization as defined in the Act.

[3] Section 36(1)(a) of the Act authorizes the Commissioner to investigate complaints and conduct investigations to ensure compliance with any provision of the Act. The Commissioner authorized me to investigate and report on this matter.

III. FINDINGS OF FACT

[4] As part of my investigation, I met with the Chief Compliance Officer of EPCOR, and with the Manager of the Customer Call Centre to review the complaints. EPCOR management provided me with the call centre scripts and procedures, and the organization's privacy policies. Subsequent meetings were held at the EPCOR offices in Edmonton and via telephone to review the organization's relevant personal information management practices.

[5] EPCOR reported that its customer service representatives collected personal information for two business purposes:

1. To **establish credit worthiness** of new customers, a \$150 deposit per utility service was requested. Complainants were told that the deposit would be returned with interest after twelve consecutive months of satisfactory payment history. If a customer did not wish to pay a deposit, the alternative of a credit check using social insurance number was offered.
2. To **authenticate individuals** over the telephone, the organization requested two forms of identification. Identification was required for all inquiries, including questions about EPCOR's overall practices, products or services. Customers were given a choice of possible forms of identification they could provide, including SIN, date of birth, driver's license number, passport number or military identification. For telephone inquiries from existing customers, staff requested confirmation of numbers that were retained in the system. EPCOR's legacy system had included Alberta Health Care numbers as a source of identification prior to January 1, 2004, but EPCOR has recently deleted this personal information from its information system in preparation for PIPA.

[6] As of January, 2004, customers calling EPCOR heard a new recorded message about the organization's commitment to privacy, which made reference to new provincial privacy legislation. This recording was immediately followed by a requirement to provide two pieces of identification; however, the message did not clearly indicate that this was a precaution to assist customer service representatives in verifying identify. As a result, complainants reported confusion and expressed discomfort with the forms of identification requested.

[7] The organization asserted that it required two forms of identification because the internally assigned customer account number was not adequate for identifying callers. The organization reported incidents and complaints involving individuals allegedly claiming to be the account holder in order to access it with nefarious intentions.

[8] Customer service staff did not clearly and consistently differentiate between the two business purposes of establishing credit worthiness and caller

authentication. While the first would require more personal information of a sensitive nature, the second function could be handled in a less intrusive fashion.

[9] Credit reporting agencies do not require an individual's SIN to provide a credit check; the SIN is an optional element. Other forms of personal information may be provided instead. However, credit reporting agencies confirm that the SIN improves accuracy and speeds up the process of obtaining a credit report.

IV. ISSUES

- [10] **1. Is it reasonable to require customers to provide a SIN for the purpose of a credit check?**
- 2. What notification and consent practices are required for the collection of personal information for the purpose of a credit check?**
- 3. If a SIN is properly collected, how should it be used? What confidentiality and security measures are appropriate?**
- 4. What forms of personal information are reasonably required for the organization to authenticate a caller/customer? Does the organization require identification from all callers, including those with only general inquiries?**

V. ANALYSIS

- 1. Is it reasonable to require customers to provide a SIN for the purpose of a credit check?**

[11] Section 3 states: *"The purpose of the Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable"*

[12] Section 11(1) states: *"An organization may collect personal information only for purposes that are reasonable"*

[13] The last part of Section 2 of the Act says: *"... the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable ... is what a reasonable person would consider appropriate in the circumstances"*

[14] Section 7(2) states: *"An organization shall not, as a condition of supplying a product or service, require an individual to consent to the*

collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.”

[15] The organization reported that there are financial risks associated with creating a new account because the customer is billed in arrears. Customers begin to receive services soon after an account is opened on credit. The organization regards establishing credit as an important business consideration for any new account. The Federal Privacy Commissioner has found it reasonable for companies to require a credit check to assess the financial risk of extending credit to individuals.¹ It is also reasonable in these circumstances for the organization to *conduct* a credit check, or, alternatively, to require a refundable deposit.

[16] The SIN was created in the 1960s to serve as a client account number in the administration of the Canada Pension Plan and Canada’s varied employment insurance programs. Employers are authorized to collect SINs from employees in order to provide them with records of employment and T slips for income tax and Canada Pension Plan purposes. Financial institutions such as banks, credit unions and trust companies are required under the Income Tax Act to ask for customers’ SINs for tax reporting purposes.

[17] No private sector organization is authorized by legislation to request SINs for purposes other than employment purposes and income reporting. However, there is no legislation that specifically prohibits an organization from asking for, and a customer providing, a SIN, as long as the organization complies with the provisions of the PIPA.

[18] The organization asserts that it is reasonable to require a SIN for this credit check because it results in a timely and accurate report. Customers who do not wish to provide their SIN for this purpose are given the option of paying a refundable deposit equal to the average cost of one month’s service. However, customers are not consistently given the option of providing alternative types of personal information (address and date of birth for example) instead of the SIN to allow for a credit search.

[19] The OIPC recognizes that the SIN is commonly used for credit checks by many private sector organizations. The Federal Privacy Commissioner has recommended that the provision of a SIN for the purpose of credit checks be optional and should not be a required as a condition of service.² Although EPCOR provided an alternative for customers who did not wish to provide their SIN for a credit check, and opening an account was not contingent on a credit check, I find that the organization should provide very clear alternatives for customers consenting to a credit check.

¹ PIPEDA Case Summary Decision #117. Credit check required for small business account applicant. Issued February 11, 2003. Principle 4.3.3 and Section 5(3). Website: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030211_e.asp.

² PIPEDA Case Summary Decision #104. Cellular phone customer objects to supplying personal information for credit check. Issued December 19, 2002. Principles 4.3.3 Schedule 1 and Section 5(3). Website: http://www.privcom.gc.ca/cf-dc/cf-dc_021219_9_e.asp

[20] I find it unreasonable for the organization to require a SIN if the credit reporting bureaus do not.

2. What notification and consent practices should be required for the collection of personal information for the purpose of a credit check?

[21] Section 13(1) of the Act states: “*Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally*

- (a) as to the purposes for which the information is collected, and*
- (b) the name of a person who is able to answer on behalf of the organization the individual’s questions about the collection.”*

[22] Section 7(1) states: “*Except where this Act requires otherwise, an organization shall not, with respect to personal information about an individual,*

- (a) collect that information unless the individual consents to the collection of that information, ...*
- c) use that information unless the individual consents to the use of the information.”*

[23] The basic requirement for organizations under PIPA is to clearly identify the purposes for which personal information is collected, and how it will be used and disclosed. Accordingly, if an organization collects information for a credit check, it must limit the collection of that information to what is required for those identified purposes.

[24] PIPA requires that personal information must be collected with consent and for a specific and legitimate business purpose. An organization must inform the individual of its purposes and obtain consent at the time of collection, either orally or in writing.

[25] In EPCOR’s case, customers were not informed of all the purposes for which their personal information would be used; therefore, EPCOR did not obtain informed consent when collecting customers’ SINs.

[26] The SIN is a sensitive form of personal information because computer technology makes it possible to use the SIN to find and match income-related and other personal information. The sensitivity of this form of personal information suggests that a more stringent standard for consent would be appropriate and that a *separate express consent* should be obtained from the individual.

[27] Prior to the investigation the organization had reviewed some of their procedures and were in the process of updating them. During the course of the investigation, EPCOR agreed to revise its notification and consent practices to clarify the purposes of collecting the SIN, and to advise customers of all uses it made of the SIN, including matching new accounts

with those in arrears. EPCOR altered its procedures as agreed, and now obtains an informed verbal consent prior to collecting SIN. I find EPCOR's revised procedures reasonable in the circumstances.

3. If a SIN is properly collected, how should it be used? What confidentiality and security measures are appropriate?

[28] Section 11(2) of the Act states: *"Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected."*

[29] While EPCOR retains the SIN for "collections" purposes; this was not included in the notification process. In the course of this investigation, the organization clarified that the SIN collected from new account holders was retained for the purpose of electronically matching new accounts with those in arrears. The organization believed this use to be justified because it helped prevent fraud and minimized financial losses. The organization asserted that the matching capability of the system (by SIN) protected the organization by identifying these individuals.

[30] Section 34 states: *"An organization must protect personal information that is in its custody...by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction."*

[31] Best practices require that organizations consider the sensitivity of the information in the circumstances when making security arrangements.

[32] EPCOR recognized the sensitivity and security risks of retaining the SIN and, during the course of this investigation, agreed to implement changes to access and security protocols to provide better protection of SINs retained in the system. I have been informed of the access and security arrangements made by EPCOR to protect SINs including allowing access to SIN information to only a limited number of EPCOR employees, and having each such employee enter into a specific Confidentiality Agreement as a condition precedent to the employee having access to the SINs. I find that the arrangements made by EPCOR in response to the concerns expressed by the complainants reasonable in the circumstances.

4. What forms of personal information are reasonably required for the organization to authenticate a caller/customer? Does the organization require identification from all callers, including those with only general inquiries?

[33] The organization reported that it is standard practice for electric utility companies to require two forms of identification for authentication purposes. The organization believes that use of personal information for authentication is effective to allow it to protect the integrity of a customer's account. The Federal Commissioner has recommended that companies who

collect information to confirm identity or perform credit checks must limit the collection of information to what is necessary for the intended purposes.³

[34] PIPA requires organizations to limit the personal information they collect to what is reasonably required to provide services and carry on business. The organization required forms of identification that many customers consider sensitive. Complainants were particularly concerned about providing or confirming their SIN. There was no differentiation between the identification required by customer service representatives for specific account inquiries and identification needed for general inquiries about services and products. The organization stated that it was most concerned about authenticating callers when the inquiry concerned a specific account (such as billing inquiries and name and address changes). The collection of identifying personal information over the phone was not limited to those transactions that actually required authentication. Also, callers were not consistently given the opportunity to provide less sensitive forms of information (such as a password or customer ID question).

[35] EPCOR has recognized the concerns expressed by complainants and other customers and has agreed to make changes to its procedures in response to the concerns. EPCOR confirmed that all Alberta Health Care numbers were purged from its system prior to January 1, 2004. Effective March 1, 2004, EPCOR established procedures to ensure that SINs would **not** be collected or used for identification purposes, and that SINs would only be used for credit checks and collections purposes after a separate express consent is obtained. Customers are not required to disclose SINs as a condition of service. Other means of establishing credit are available, including the option of providing a refundable deposit. I find the revised procedures to be reasonable in the circumstances.

[36] EPCOR has agreed to review its Customer Services privacy procedures and to provide a compliance report to the OIPC, at a time satisfactory to the OIPC.

VI. RECOMMENDATIONS

[37] I make the following recommendations to conclude the issues raised in this investigation:

1. EPCOR to review the posting of privacy policies and other communications forms. Ensure adequate training exists for front line staff that addresses responsibilities under the PIPA. Improve the means by which individuals may contact a company representative who can answer detailed or complex privacy inquiries.

³ PIPEDA Case Summary Decision #202. A Telecommunications company requires two pieces of identification from a new subscriber. Issued August 5, 2003. Principle 4.3.3, principle 4.4 Schedule 1 Subsection 5(3). Website: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030805_06_e.asp

2. EPCOR to develop a standard script and procedure for notification and obtain a separate express consent when collecting SINs. Limit the use of SINs to those purposes specified at the time of collection.
3. EPCOR to develop a procedure to ensure that the provision of SINs for the purpose of credit checks is optional.
4. EPCOR to ensure that the confidentiality of customers' sensitive personal information is protected by limiting access to this information. Since SINs are no longer used for authenticating callers, they should not be visible on the system to call centre staff.
5. EPCOR to develop a procedure that gives the customer a choice of which elements of identification are provided for authentication purposes. Ensure that the options are presented beginning with the least sensitive type of personal information (e.g. a customer's selected password or question). Ensure that all call centre scripts list the order of these identifiers in a consistent manner.
6. EPCOR to develop a procedure that allows an individual to opt out of submitting personal information over the telephone for the purpose of authentication and forewarn that this may require that individual to visit the EPCOR offices in Edmonton. Adjustments to accounts may only be made after reasonable identification is produced.
7. EPCOR to review privacy policies and procedures in relation to customer information and prepare a compliance report describing the organization's progress in implementing the recommendations in this report, to be filed with the OIPC on or before September 30, 2004.
8. EPCOR to conduct a privacy audit in relation to customer information procedures (in Alberta), and the organization's compliance with PIPA.
9. EPCOR to monitor and review the practice of collecting SINs for the purpose of a credit check in light of public views and jurisprudence in the matter.
10. EPCOR to provide quarterly reports to the OIPC on compliance activities related to this investigation (for a one year period).

VII. CONCLUSION

[38] EPCOR's privacy practices were not in compliance with its obligations under PIPA regarding Notification, Consent, Limiting Collection, and Limiting Use in relation to customers' social insurance numbers. The organization has taken, or has committed to take, appropriate action by developing new procedures, conducting training for front line staff, and implementing significant changes to its information systems.

VIII. COMMENTS

[39] EPCOR took appropriate corrective action during the course of this investigation. I thank EPCOR for cooperating fully with this investigation and for its commitment to change practices in response to the complainants' concerns.

[40] This file is now closed.

Submitted by:

Elizabeth Denham
Private Sector Lead
Office of the Information and Privacy Commissioner of Alberta