Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Language of consent and monitoring activity challenged

PIPEDA Case Summary #2005-296

(Principles 4.3 and 4.3.2; subsection 5(3))

Complaint

An individual alleged that the language of a credit card application form outlined overly broad collection, use and disclosure practices, and therefore did not meet the requirements for consent. The complainant also alleged that the bank was inappropriately monitoring the purchasing history of cardholders.

Summary of Investigation

The complainant felt that the definition of personal information contained in the section of the application form pertaining to uses of personal information was too broad. The form stated that personal information was any information that related to an individual and allowed that individual to be identified. The complainant argued that the form should clearly set out the categories of personal information that is collected, and that these categories should be limited to personal contact and financial information.

The bank, however, pointed out that its definition was consistent with the meaning of personal information under the *Personal Information Protection and Electronic Documents Act* (the Act). The bank believed that it was not obliged to enumerate every type of personal information that it collects; rather, its obligation was to identify the purposes for which personal information is collected, and limit the collection to that which is necessary for those purposes.

The bank's purposes for collecting personal information were included on the application form. They were as follows:

- To develop and maintain a business relationship with its customers, and to analyze and manage its business
- To administer customer billing and accounting services, and security measures
- To monitor customer purchasing history
- To evaluate the customer's credit standing
- To comply with legal and regulatory requirements
- To promote and market products and services (optional).

The bank indicated that it was not possible, given the nature of the service that it offers, to limit its collection activities to personal contact and financial information. It stated that each time a customer uses a credit card, the bank collects information about the financial transaction (the amount of the purchase), but it also collects such information as the type of product purchased, and the time and location of the purchase. The bank also pointed out that it is required by law to

collect more than just personal contact information. For example, it must collect the applicant's date of birth to verify identity and to fulfil the bank's regulatory obligations under the anti-money laundering and terrorist financing legislation. (Section 67 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires banks to record the date of birth of the individual on the account application form.) The complainant nevertheless maintained that the bank must clearly define the scope of information that it intends to collect in advance of the collection.

The complainant also took umbrage with the application form's language of consent concerning collection, use, and processing of personal information, believing that it was far too broad, and could conceivably permit the bank to collect more information than necessary.

The bank stated that it makes two other documents, in addition to the application form, available to customers, which address this concern. Its privacy code indicates that the bank only collects customer information that is needed and that the bank tells customers how it uses it. The other document is a declaration that is part of the account agreement form. It sets out a customer's privacy rights, including the right to access all personal information held on file, and to correct it as appropriate. The bank stated that an account holder who is concerned that the bank might be collecting more information than necessary for its stated purposes would be able to confirm or allay his or her suspicions by reviewing the bank's actual practice in the context of an access request.

The complainant was also concerned about another consent clause that referred to the sharing or exchange of reports and information with credit reporting agencies, credit bureaus and/or any other person, corporation, firm or enterprise with whom the customer has or proposes to have a financial relationship. In the complainant's view, this section described a broad-based list of potential recipients of his personal information and that the range of potential recipients is so broadly described that it suggests that the bank is acting as a credit bureau.

The bank felt that the complainant had taken the wording of the consent provision out of context. As it is granting credit, the bank wants to ensure that it covers those financial relationships that would be appropriate to verify credit standing. It pointed out that customers change their banks and other financial relationships over time, and this provision allows it to continue to service the account and evaluate the customer's credit standing. Furthermore, the bank indicated that its consent provisions must be viewed in the context of the appropriate purposes that it has set out for the collection, use and disclosure of personal information. The complainant agreed that this position was reasonable, but believed it should be reflected in the language of the consent form. The bank's privacy code gave a better description of its disclosure policy.

Of the purposes outlined by the bank for collecting, using or disclosing personal information, the complainant was most concerned about the requirement that he consent to the monitoring of his purchasing history. He believed that such an action was tantamount to corporate surveillance. In his opinion, monitoring should be focused exclusively on the detection of fraudulent activity, and he questioned whether the bank monitors its customers' purchasing history for secondary purposes. If so, the bank should clearly indicate this and make such consent optional. The complainant was concerned about the potential for details of customer purchasing history being inappropriately disclosed to a third party.

The bank stated that it monitors customer purchasing history for three reasons: to identify a credit risk (where the customer is using credit excessively); to identify a fraud risk for the benefit of the customer and the bank; and to fulfil the bank's regulatory responsibilities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. The bank's privacy code uses somewhat different language to describe this purpose, indicating that it collects, uses and discloses personal information to detect and protect the bank against error, fraud and other criminal activity.

Findings

Issued March 14, 2005

Application: Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate; Principle 4.3.2 indicates that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information shall be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed; subsection 5(3) states that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

In making her determinations, the Assistant Privacy Commissioner deliberated as follows:

- She generally found the purposes for collecting, using and disclosing personal information to be appropriate, as per the reasonable person test outlined in subsection 5(3). Where the purpose is indicated as optional, a customer could easily indicate that he or she did not want to be solicited for other products, at the time of application.
- The Assistant Commissioner was not, however, satisfied with the language used to describe the scope of information collected and disclosed. A customer, she stated, should not have to make an access to personal information request of a bank to find out what information has been collected or disclosed. Rather, she noted that banks should provide examples up front of the kinds of personal information collected, such as name, address, language preference, birth date, employer, occupation, credit rating, value of investments held, and repayment history on loans. They should also outline a rationale for the collection of each type of information (for example, the collection of birth date is required by law).
- The complainant had singled out monitoring of customer purchases as an area of concern. While the Assistant Commissioner believed that such an activity was appropriate for the purposes of detecting fraud and criminal activity, and reviewing credit use, she agreed that an individual would not understand from the language of the application form or from the other privacy-related documents why the bank monitors purchasing history.
- Thus, while she was satisfied with the bank's stated purposes, she believed that the bank was not providing meaningful consent with respect to its collection, use and disclosure practices, as required under Principles 4.3 and 4.3.2.

The Assistant Commissioner concluded that the complaint regarding the purposes for collection, use and disclosure was not well-founded (/en/opc-actions-and-decisions/investigations/def-cf/), but the complaint regarding the language of consent was well-founded (/en/opc-actions-and-decisions/investigations/def-cf/).

Further Considerations

The Assistant Commissioner made the following recommendations:

- That the bank revise the portion of the application forms concerning the monitoring of purchasing history to provide applicants with adequate information concerning this activity
- That the bank take steps to include in its privacy materials more detailed information regarding the types of personal information it collects and to link the type of information collected to its use
- That the bank report back to her on its implementation of these recommendations.

The Assistant Commissioner also took the opportunity to comment on two other issues that arose during the course of the investigation.

1) The form indicates that the applicant should allow eight to ten weeks for an "opt-out" request to be processed. In other similar complaint findings made by this Office, we took the position that new applicants for a credit card should be able to opt-out immediately, at the time of application, from all secondary uses of their personal information.

The Assistant Commissioner relayed recommendations the Office has made to other banks regarding their application forms, which she considered useful. Specifically, we have recommended that the form indicate that:

1. A customer does not have the option of withdrawing consent to the bank's disclosure of credit information to the credit bureaus
2. Banks should include a statement of purpose for the ongoing disclosure of credit information to the credit bureaus (i.e., to maintain the integrity of the credit granting system)
3. The collection of name, address, date of birth, and occupation of the applicant are required by law.

The Assistant Commissioner urged the bank to also include such information on its application forms.

2) Finally, the complainant raised a concern about the size of the font used on the application form. After considering the matter, the Assistant Commissioner was satisfied that there are a number of important decisions involved in choosing the size of the font used and that privacy has not been diminished since other important account information is also in the same sized font. In recognition that there are limitations to the amount of text that can be included on an application form, she recommended that the bank include a statement on its form drawing the applicant's attention to resources that provide more detail about its privacy practices, such as its privacy code, available on its web site or through its toll-free number.

Date modified:

2005-04-20