



CBA Submission to House of  
Commons Standing  
Committee on Access to  
Information, Privacy and Ethics  
on Five Year Review of  
Personal Information  
Protection and Electronic  
Documents Act

Prepared by the Canadian Bankers Association

January 2007



CANADIAN BANKERS ASSOCIATION

*Building a Better Understanding*



## Introduction

The Canadian Bankers Association welcomes the opportunity to provide the banking industry's comments and suggestions regarding the *Personal Information Protection and Electronic Documents Act* (the "Act") as the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee") begins the legislated five-year review of the Act. Our comments below provide a brief background on the banks' experience with the Act, our views on several substantive issues that we suggest should be addressed, suggestions for amendments to harmonize with provincial laws and the industry's views on issues that have been raised by other stakeholders.

## Protection of Personal Information in the Banking Sector

The banking industry has been a leader in Canada in the protection of personal information. Banks recognize that privacy and confidentiality of personal information, and particularly their personal financial information, is a high priority for Canadians. Privacy has always been a cornerstone of banking, and strong measures to protect personal information have long been embedded in the banks' policies and practices.

The banking industry was the first industry in Canada to publicly set out its commitment to privacy protection by codifying its policies and practices in a detailed privacy code, first introduced almost 20 years ago. That code was modified several years later and again in 1996 to conform to the Canadian Standards Association *CAN/CSA-Q830-96 Model Code for the Protection of Personal Information: A National Standard of Canada* (CSA Model Code). The CBA model code, the first code to be confirmed as complying with the CSA Model Code, was superseded by the Act in 2001. The banks, as federally regulated financial institutions, were among the first federal works, undertakings and businesses subject to the Act in January 2001.

While the Act used the CSA Model Code principles as the basis for the legislative requirements, the legislation did introduce new requirements and modifications of the CSA Model Code principles that required businesses, including the banks, to re-examine how they implemented privacy protection within their operations. Adjustments were required and implemented and the banks' policies and procedures continue to demonstrate the industry's leadership in and commitment to strong privacy protection.

Canadian banks work hard to prevent their operations and customers' personal information from being used for any kind of financial crime, ranging from scams, identity theft, deceptive telemarketing and debit and credit card theft to money laundering. Their efforts include employee training and rigorous internal process and procedures, customer awareness programs and cooperation with governments, law enforcement agencies, and other bodies at both the national and international levels. The banking industry expends great efforts and expense to prevent, detect and deter fraud and other crimes against banks and their customers, including criminal activity resulting from identity theft.

Protection of our customers' and employees' personal information is paramount. Nevertheless, when handling over 11 million transactions each day for our customers, errors can and do happen. The banks' goal is to minimize such errors and ensure that they do not recur. Considering the almost daily interactions that

customers have with their banks, the relatively small number of privacy complaints that have been taken to the Privacy Commissioner provides strong evidence of the banks' success in protecting personal information.

Generally the banks are of the view that the Act has served Canadians well in protecting the personal information collected, used and disclosed about them by private sector organizations and, from an organizational perspective, has provided the necessary structure to allow private sector organizations to effectively implement its requirements into their business operations. There are nevertheless a few areas where amendments to the Act could provide consumer benefits, improve clarity and address gaps that have become apparent.

## **Disclosure without consent when in the public interest**

Situations arise, both with banks and other organizations, where the current requirements of the Act prevent employees from acting in the interests of the greater good of an individual or group of individuals. An example of such a situation in the banking context is where a banker suspects financial abuse, particularly with seniors, when a customer is withdrawing money from his or her account. It appears that the customer may be under pressure from the person accompanying him or her, or that the withdrawal is uncharacteristic of the person. Under the current legislation, the banker suspecting abuse is precluded from disclosing information about the transaction to the authorities, the vulnerable customer's family or another responsible person who might be able to investigate and stop any abuse.

Elder financial abuse is a significant issue in Canada. Data from the General Social Survey on Victimization conducted in 1999 by Statistics Canada showed that approximately seven per cent of seniors reported they had experienced some form of emotional or financial abuse by an adult child, caregiver or spouse in the five-year period preceding the survey. Financial abuse is the most common form of abuse and can include misappropriation of funds, improper use of power of attorney forms and other frauds and scams.

Prior to the Act coming into force, bankers had a common law right (*Tournier* decision) that allowed disclosure without consent when it was in the public interest. This was generally used by the banks to address situations such as the abuse described above. Bankers still feel that obligation, and are frequently under pressure from public interest groups and public authorities, to act on their suspicion and report the suspected abuse to another family member or the authorities. Both British Columbia (BC) and Alberta legislation define "legal proceeding" to include remedies "claimed ... under the common law or in equity", or "available at law" (see Definitions in both statutes). Yet s. 7(3) of the Act does not allow such disclosures without the customer's consent, which is difficult to request in this type of situation.

Another example in the banking context would be where there has been a natural disaster (such as the 2004 tsunami or the Bali bombing) where family members want to determine whether a loved one has survived and seek information about whether there is activity on a credit card or other account as an indication that the person is still alive.

The banks' capacity to act on matters of public duty, within the parameters of the common law precedent, is useful for banks and their customers alike. It should be noted that this common law duty to protect the public interest does not by any means absolve banks of the need to treat their customers' information responsibly. It

simply acknowledges that individual rights, including privacy rights, may occasionally conflict with one another, or with the broader public good.

There are also situations in the employment context where the employer needs to convey important information to an employee but cannot locate that employee and needs to contact the next of kin or designated contact.

While s. 7(3)(e) allows disclosure “to a person who needs the information because of an emergency that threatens the life, health or security of an individual”, it does not appear that this provision would capture the situations encountered above. Moreover, while reprehensible, financial abuse often does not contravene any existing laws. We would recommend that the Act be amended to accommodate disclosures to appropriate parties when it is in the public interest.

We would recommend that s. 7(3) of the Act be expanded to permit disclosure of personal information to appropriate authorities, the next of kin or a designated contact for the individual when the release of that information would be in the individual's or the public's interest.

## **Investigations**

The Act should be amended to follow the approach of the BC statute that, instead of designating investigative bodies, allows collection, use and disclosure of personal information without knowledge or consent for the purposes of an investigation. Such a change would not only address the inconsistencies between the exemptions for collection, use and disclosure (subsections 7(1), 7(2) and 7(3)) described below, but also the administrative burden on the Government to open up the regulations every few months to add more approved investigative bodies to the list.

There are inconsistencies between the exemptions for collection, use and disclosure in the Act that can make it difficult for the banks to prevent fraud against their customers, other customers and the bank. In their efforts to prevent and investigate fraud against their customers and the banks themselves, banks frequently encounter situations where they need to be able to collect, use and disclose personal information without consent but are unable to do so due to the Act's inconsistencies among sections 7(1), 7(2) and 7(3). For instance, while the Act allows an organization to collect and disclose information relating to a breach of an agreement, it does not allow for internal use of that same information in the course of the investigation to prevent further fraud against that customer, other customers or the bank.

Similarly, a bank investigating a fraud could find and use internally information suggesting contravention of a foreign law but would be unable to collect any further information to confirm that suspicion. It could even disclose that information to the Bank Crime Investigation and Prevention Office (BCPIO) but the BCPIO could not do anything with that information because it is not able to disclose information relating to contravention of a foreign law, even to local authorities or other local organizations that might be similarly impacted. This causes significant barriers to investigating and preventing further crimes against a broader cross-section of the industry.

The BC statute includes “prevention of fraud” as one of the acceptable components in its definition of “investigation” (s. 1 Definitions). While the Act currently does not define “investigation”, perhaps this concept could usefully be applied in the Act to provide greater ability to organizations to assist with the prevention of fraud.

In the Act, “investigation” needs to be clarified to ensure that it includes and allows the full range of necessary and desirable circumstances that might prompt an investigation. Both the BC (s. 1) and Alberta (s. 1(f)) statutes allow investigations related to a breach of an agreement, contravention of a law, prevention of fraud, and “circumstance or conduct that may result in a remedy or relief being available under an enactment, under the common law or in equity” (BC *Personal Information Protection Act*).

We would recommend that the Act be amended to harmonize with substantially similar provincial legislation to define “investigation” so that the full range of acceptable circumstances found in provincial legislation are clearly included under federal law.

## **Exemptions to access rights**

Since the coming into force of the Act in 2001, its access provisions have been used by some individuals<sup>1</sup> to circumvent or subvert legitimate business processes and activities in ways not intended by the Act. Access requests should be used for legitimate privacy purposes and not used to thwart other legitimate legal or business transactions, nor for frivolous, vexatious or trivial reasons or in bad faith. There are also circumstances where additional protection for personal information held by organizations is required. We believe that specific measures need to be included in the Act to address the access concerns that are enumerated below.

### **a) Circumventing legal due process**

Some individuals have used the access rights under the Act to obtain information related to a legal proceeding. Documents created for the purpose of litigation are privileged and do not need to be provided to other parties under the rules of court (Litigation Privilege). The current wording of s. 9(3)(a) would appear to allow access to these documents. An amendment is required to allow for access to be refused if information is protected by a privilege recognized by law. The Alberta legislation addresses this aspect in s. 24(2)(c), providing an exemption when “the information was collected for an investigation or legal proceeding”.

The CBA recommends that the Act be amended to clarify that organizations may decline an individual’s request for access to personal information where the information was collected for an investigation or a real or anticipated legal proceeding.

### **b) Protecting investigation information**

While s. 9(3)(c.1) exempts information collected under s. 7(1)(b) to investigate a breach of an agreement or contravention of laws, the exemption is not broad enough to capture information collected for normal business transactions but subsequently related to an investigation. An example of this situation might be when a bank

---

<sup>1</sup> These individuals could be customers or employees, current or former.

is investigating an alleged kiting or embezzlement scheme and collecting information about a customer's or employee's past transactions. If the individual were to be made aware of the bank's aggregation of this particular information, it could conceivably hinder the investigation and prevent apprehension of the perpetrator. The Act provides for an access exemption for information collected for an investigation but not for information that is being used for an investigation. The exemption in s. 9 (3)(c.1) should be broadened to include all information that if released might hinder an internal investigation into a breach of an agreement or contravention of laws.

The CBA recommends that the Act be amended to clarify that organizations may decline an individual's request for access to personal information where providing access might hinder an internal investigation into a breach of an agreement or contravention of the laws of Canada or a province.

**c) Circumventing normal legitimate fees**

Bank customers wanting replacement copies of documents already provided to the individual will often make an access request to avoid the standard replacement statement fee. While the simple replacement of a statement does not constitute a significant abuse, other requests do appear to be an abuse of the Act's intent. For instance, customers who have not retained statements and other records and where due to a government audit need a number of years' worth of statements and receipts will use the access provisions to avoid paying the significant costs the bank must incur to retrieve the requested information. Similarly, an estate executor who is missing records of the estate will often seek several years' worth of statements to assist with finalizing probate of the estate and again may use an access request under the Act to avoid paying to retrieve this information. These and similar uses of the Act are not related to privacy protection and the access requirements should not be used to avoid payment of reasonable costs for retrieving the information.

The CBA recommends that the Act be amended to clarify that organizations may charge reasonable costs to provide an individual with access to personal information where the information was previously provided to the appropriate individual and is typically provided for a fee.

**d) Substantive access**

The banks support the principle of access and make every attempt to comply with the spirit and the letter of the law in this regard. Given the nature of large complex organizations like banks, however, it is virtually impossible for a bank presented with a request for all information about an individual to fully comply with that request.

A customer who provides the bank with full information about the range of his or her relationship with the bank (all the bank products and services they use) will certainly be provided with all the information associated with those products and services. There maybe other details, however, such as lists provided to distribution agents that mail statements or other similar routine processes associated with the normal operation of an account, that are buried in the operational processes and not able to be retrieved without significant effort and expense, or at all. Given that the individual is not likely to consider this type of information to be relevant to the access request, it would be helpful if the Act were to clarify that an access request is deemed to have been fulfilled if the substantive information has been provided.

Moreover, the cost of conducting a search for personal information should be a relevant factor when determining if an organization has met its obligations pursuant to an access request. The organization should be held to a reasonable standard in conducting a search as opposed to a “perfect” search in order to meet the access request obligations.

The CBA recommends that s. 9(3) be amended to deem an access request to have been fulfilled if the substantive information related to the individual’s relationship with the organization has been provided and where providing further non-substantive information would result in a considerable cost to the organization. We would recommend that there be a specific exemption for requests for access to personal information that has otherwise been addressed in a reasonable fashion.

**e) Trivial, frivolous and vexatious requests**

Organizations on occasion receive repetitive and apparently systematic requests for access to the personal information they hold about individuals. In many cases, it appears that these requests are such that they could be categorized as “trivial, frivolous, vexatious or made in bad faith”, characteristics that the Act recognizes as sufficient to allow the Commissioner to avoid preparing a report about a complaint. Organizations would be better able to serve those consumers with legitimate needs for access if the Act provided an exemption for the less legitimate requests that appear to abuse the right to access. Consumers would, of course, continue to be able to appeal refused access requests to the Commissioner.

The CBA recommends that s. 9(3) be amended to clarify that organizations may decline an individual’s request for access to personal information where the request abuses the right to access, being frivolous, vexatious or in bad faith having regard to a multiplicity of factors.

## **Recourse when differing views regarding access request**

The Act in s. 9(3) recognizes amongst other provisions, the solicitor-client privilege, commercially sensitive information and the sanctity of information held as part of a formal dispute resolution process, and therein provides exceptions to the individual’s right to access. The Commissioner may, as part of her investigation into complaints about an organization’s denial of access, collect the disputed information to assist with its determination as to whether that information should be exempt from access. Notwithstanding an organization’s strong belief that the information is subject to legal privilege, commercially sensitive or germane to a formal dispute resolution process, the Commissioner may find that the information is not so exempt and should be provided to the individual.

If, despite the Commissioner’s finding, the organization continues to believe that the exemption should apply and the organization is prepared to appeal the finding in the only way open to it – that is by not complying and thereby perhaps forcing the Commissioner to take the action to the courts – it should be clear in the Act that the Commissioner does not have the right to release the disputed information in her possession prior to a court decision.

The CBA recommends that the Act be amended to clarify that the Commissioner must hold confidential any personal information collected as part of an investigation or protected by privilege or that is commercially

sensitive and, notwithstanding a finding to the contrary, respect an organization's views that an access exemption applies until such time as a court rules otherwise.

## **Sharing information within corporate groups**

Many corporations that have multiple separate subsidiary companies as required by federal/provincial regulatory requirements nevertheless operate as one unit under a single management team. The banks are no exception, since the business of banking is federally regulated and, for example, the insurance and securities businesses are under provincial jurisdiction. There are other laws, however, that require that the banking group operate and report as one unit.

One example is with Basel Capital Framework, where the compliance function must look across the entire organization to determine the total banking group's exposure to certain borrowers. Similarly with anti-money-laundering requirements, the banking group must look at the activities of each customer across their dealings with the entire banking group, not just each entity separately. In the securities field, related parties assessments must include information from all parts of the financial group, not each entity separately.

These other legislated requirements require that information about individuals be communicated and aggregated at the corporate group level, but appear to conflict with PIPEDA's requirements not to share information with different parts of the corporate group. Amendments to PIPEDA that would acknowledge these other legislative requirements and facilitate required regulatory reporting would be desirable.

The CBA recommends that the Act be amended to recognize other regulatory requirements and facilitate regulatory reporting as a corporate group.

## **Federal-Provincial Harmonization**

When drafting the BC and Alberta laws which have subsequently been judged substantially similar to the Act, provincial drafters had the benefit of being able to refer to and use desirable provisions from the Act, and to learn from the first few years of experience in implementing it to incorporate enhancements in their legislation. Generally the provincial statutes are clear and practical and reflect an updated reflection of privacy protection today.

This five-year review of the Act gives federal policy makers and legislative drafters the same opportunity to use the provincial experience to enhance and update the Act. We encourage a general review of the provincial statutes and, where they provide additional clarity, use of those provisions. The most important areas for clarification from the banking industry's perspective are highlighted below.

### **a) Expand definition of business contact information**

Since the Act was passed, information technology has resulted in considerable expansion of the use and variety of communications technology used in the business context, a good current example being e-mail. It is critical now that the Act be updated to allow employers to disclose employee business e-mail addresses

and business fax numbers so that customers and others can communicate with employees. Moreover, to allow the Act to accommodate future innovations in business communication, the Act should allow for “other similar business information” to be disclosed as is found in the Alberta statute in s. 1(a).

The CBA recommends that the Act be amended to harmonize with substantially similar provincial legislation to define “personal information” to exclude all business contact information, including business e-mail and business fax numbers as well as “other similar business information” to allow for future business communication technologies to be accommodated.

**b) Collection and use without consent for collecting or paying a debt or enforcing an obligation**

Section 7(3)(b) of the Act currently provides for disclosure without knowledge or consent for the purpose of collecting a debt owed by the individual to the organization. An organization attempting to collect on a debt needs to obtain additional information as to the borrower’s current whereabouts or the location of goods pledged as security for the loan (car, boat, etc.) and to use all information available to collect an outstanding debt. We recommend that similar exemptions be provided for both collection and use, and also for the repaying of a debt. Such provisions were incorporated in the BC and Alberta laws (sections 12(1)(j) and 14(i) respectively).

We also recommend that the Act be amended to expand “collecting a debt” to also include “enforcing an obligation” owed by the individual. This minor change is necessary in order to allow for the enforcement of obligations that may not be classified as debts, such as the obligation to keep a mortgaged property in good repair, the collection of overdue taxes payable under a mortgage loan, where a bank seeks to recover property that is subject to a security interest, where an organization is commencing proceedings to obtain an injunction, a reimbursement obligation under a letter of credit, and an indemnity given in connection with the replacement of lost cheques.

The CBA recommends that s. 7 be amended to provide the ability for organizations to collect, use and disclose personal information without consent for the purposes of collecting a debt or enforcing a contractual obligation owed by the individual to the organization, or for the purposes of paying a debt owed by the organization to the individual.

**c) Mergers, acquisitions and securitization**

In the event of a purchase of all or part of the assets or shares of one organization by another, the purchasing organization needs to be able – in advance of any decision and in complete confidence – to conduct the necessary due diligence to assess the purchase and, in so doing, would examine files that may include personal information of customers and employees. The parties to such contemplated transactions are typically bound by contractual restrictions regarding the confidentiality of the information that is disclosed. In addition, employees are often an important element of the business being acquired and the potential purchaser will often want and need information about the employees so as to be able to present an attractive offer to those employees that it intends to retain. It would be inappropriate for the affected individuals whose information was being accessed to be informed under these circumstances. Moreover, with respect to employees, if consent is required prior to information being disclosed to the purchaser, there will be a delay in analyzing the information from that point to the date on which offers can be presented to employees, during

which employees will be in a state of uncertainty – which is very counterproductive to the interests of all parties, including the employees.

If the purchase went ahead, all personal information related to the assets being transferred would then be disclosed to and ultimately used by the purchasing organization. Examples of such a situation might be a bank selling off certain operations, assets or a product line; or a bank buying another financial institution. The Alberta privacy legislation (s. 22) included some desirable provisions relating to business transactions to accommodate the collection, use and disclosure of information related to corporate restructuring and business transactions such as mergers and acquisitions and securitization of assets. We recommend that the Act be amended to similarly acknowledge and facilitate such business transactions.

In the case of banks and others covered by the *Proceeds of Crime (Money-Laundering) Regulations*, however, there is a requirement that an organization retain certain information for a period of five years after closing an account or terminating a relationship. Following a sale, while the vendor is no longer the owner of the information, it may hold some personal information strictly for regulatory compliance. Nevertheless, any information held by the vendor organization is strictly for regulatory compliance so any access request should be directed to the new owner of the information. There should therefore be a restriction on access rights for the individual, in that the individual should not be able to obtain access to their personal information except through the new owner of the business, which then holds the information.

We would recommend that the Act be amended to include an exception for consent similar to that used in the Alberta statute that would specifically allow for the transfer and use of personal information processes involved in examining the feasibility of and effecting business activities such as corporate restructuring, securitization and the sale of business assets.

**d) Correction of opinions, including professional or expert opinions**

The Alberta statute in s. 25(5) specifically exempts opinions, including professional or expert opinions, from being corrected or altered. In the banking context, loan decisions are often based on opinion, as are property appraisals and environmental reports are regularly obtained for the bank's use in assessing whether the bank provides a loan. Notwithstanding that the loan applicants may not agree with the opinion or content of the reports, there should be no obligation on the part of the bank to amend these expert opinions.

The CBA recommends that the Act be amended to specify that organizations are not obligated to amend opinions, including professional or expert opinions.

**e) Collection of information in individual's interest**

In the commercial context there are many situations where information about an individual is collected from someone else in order to benefit that individual. Examples include the name and address of the recipient of a delivery (the florist collects Mom's name and address to deliver flowers on Mother's Day); insurers collect the address and driver's license for spouse and dependent children driving the family car; lawyers collect the name and identifying information about the beneficiaries of wills, insurers collect information about the beneficiaries in insurance policies and banks collect information about RRSP/RRIF beneficiaries. The Alberta statute in s. 14(a) allows for the collection of information without consent when it is in the interests of the

individual and the individual would not reasonably be expected to object. This would be a desirable enhancement to the Act.

The CBA recommends that the Act be amended to provide that an organization can collect personal information about an individual when it is to the individual's benefit and the individual is not likely to object.

**f) Access might preclude collection**

The Alberta statute provides a valuable exemption from access in s. 24(2)(d) where it exempts situations where “the disclosure of the information might result in that type of information no longer being provided to the organization when it is reasonable that that type of information would be provided”. This situation would arise, for example, in the employment context with references for potential hires, or in the whistle-blowing context where retribution may be feared.

The CBA recommends that a provision be added to the Act to exempt access in situations where the disclosure may result in information no longer being provided to the organization when it is reasonable that that type of information would be provided.

**g) Disclosure to self-regulatory organizations**

Increasingly organizations are governed by self-regulating organizations (SROs) and subject to the rules and requirements they establish in lieu of government regulation. Examples in the financial sector include the Investment Dealers Association of Canada and the Mutual Fund Dealers Association. As part of their market conduct oversight responsibilities, SROs require that information about complaints from individual customers be provided to them. Customer consent may not always be sufficient or possible. The Alberta statute in s. 20(n) recognizes that organizations must be able to disclose information “for the purposes of protecting against, or for the prevention, detection or suppression of, fraud, market manipulation or unfair trading practices” where “the organization that is disclosing the information or to which the information is being disclosed is permitted or otherwise empowered or recognized under an enactment ... to carry out any of those purposes.” A similar provision in the Act would be desirable.

Alternatively, if SROs could be defined as a government institution or part of a government institution, then s. 7(3)(c.1)(iii) would apply. Or s. 7(3)(l) could be expanded to say “required **or permitted** by law.”

The CBA recommends that a provision be added to the Act to facilitate the disclosure of required information to self-regulatory organizations.

## **Commissioner's Powers**

The banking industry believes that the current ombudsman model for the Office of the Privacy Commissioner of Canada (OPCC) is effective at balancing the rights of individuals to protect their personal information and the rights of organizations to use that information in legitimate ways for their commercial purposes. The ombudsman model allows the OPCC to work with both consumers and organizations to help them better understand what is – and is not – required to achieve the ultimate goal of privacy protection.

By far the majority of organizations welcome the opportunity to work with the OPCC on a collaborative basis to bring about better compliance. The OPCC's ability to publicly identify organizations and/or to pursue legal remedies in the federal courts provides a powerful incentive to comply and the means to compel compliance, if required. The Commissioner already has powers such as audits, Commissioner-initiated complaints and other types of investigation, litigation and naming recalcitrant organizations, none of which have been used as yet to any significant degree.

In the commercial context, an organization's good reputation is the cornerstone of its success and, if ever seriously damaged, is difficult to recover. Consumers value their privacy and want their personal information protected. In today's competitive marketplace, many consumers will switch to a different organization if they feel their personal information is not being protected properly. Thus the Commissioner's ability to publish the names of organizations provides a serious incentive for most organizations to comply.

If the Government determines that changing the nature of the Commissioner's powers is desirable, it should recognize that such a change would be a complex exercise that would affect other roles of the OPCC – mediation, education and audit, for example – and require a reconsideration of the role of the Federal Court under the Act. As such, the implications of this change should be thoroughly researched and considered, which would require more time, in our view, than is available during the current review of the Act. This type of change should be deferred until the next review of the Act in order to provide sufficient time to consider the issue in depth.

## **Naming Names**

Some stakeholders have suggested publicly that the Act should require the Commissioner to name the organizations in all the Commissioner's findings. Proponents of this position suggest that it would promote fairness, market efficiency, compliance, accountability and oversight.

While the banking industry supports the principles espoused by these stakeholders, we do not believe that publication of the names of every organization in every instance where they have been found by the Commissioner not to be complying with the Act is either fair to the organization or of true value to consumers. Publication of every failure to comply with privacy requirements could have an unjustified but significant and negative effect on that business' reputation and could in fact mislead consumers.

Where there is a significant concern about how a business is treating personal information and significant impact on consumers, publication is indeed an excellent mechanism for ensuring compliance and punishing offenders. This can be judged by the Commissioner to meet the public interest requirement that is already available in the Act. Where there has been a minor error by one staff member, or where an organization has corrected the error and consumer interests have not been harmed, then in our view there is little merit in raising unnecessary concerns about the organization as a whole with the public.

Publication of the name of an organization found to have abused privacy protection requirements should be a notable announcement to which the public's attention is drawn. If every minor contravention of the Act is published with the name of the organization, the public will become inured to the announcements and not pay attention to announcements when there are serious implications for individual privacy.

The banking industry advocates maintaining the status quo, where the normal practice is that Commissioner's findings are released without the organization being named. This provides the necessary guidance to organizations as to interpreting the requirements of the Act (the original purpose of publishing the Commissioner's findings) while reserving punishment for the most egregious contraventions of the Act. Organizations should only be named in the most serious situations of a systemic nature where consumers need to know about the breach to protect themselves or where the organization has refused to correct the breach. The current process is successful as it has been implemented, with the Commissioner naming organizations following investigations where it is perceived to be in the public interest.

## **Blanket Consent**

One of the basic principles of privacy protection as outlined in Schedule I of the Act is that the knowledge and consent of individuals are required before their personal information can be collected, used and disclosed. Our interpretation of what is required by "knowledge" is that individuals should be made aware of the purposes for which the information is being collected and that they should be able to anticipate how the organization plans to use and disclose personal information about them.

The information provided to individuals should be sufficiently specific that any uses and disclosures should not be surprising to the individual. For example, if a bank indicates that it would like to use the information to market products and services of its related subsidiaries which include mortgage, investment and securities firms and the customer consents, the customer should not be surprised to receive marketing information from that bank's investment subsidiary.

Commercial organizations are called upon to balance a number of priorities in the customer interface, one of the most difficult being customers' expectations for fast service and no wait times with the need to provide them with sufficient information to ensure both that they understand and are ultimately satisfied with the product or service being purchased and that the bank is meeting its multiple regulatory requirements. Longer, more detailed disclosures to customers would negatively affect customer service and exacerbate the existing customer perception that disclosures and agreements are long and complex. Any requirement to obtain specific consent for every aspect of a relationship would be viewed negatively by most customers.

As long as the individual giving the consent understands the purposes for which the consent is given and the uses and disclosures are consistent with the stated purposes, they should be given the ability to give a broad consent. Many individuals welcome the service that can be provided by organizations that know more about them and use their information to provide better service. As long as the individual can limit or withdraw consent to additional uses, the discretion should be the customer's.

## **Duty to Notify**

The banking industry supports the need for organizations to notify individuals if an internal investigation concludes that there is a reasonable risk that their personal information could be misused for fraudulent purposes or identity theft. We strongly believe that this is the right thing to do to protect the individuals whose

information we hold. This is also the standard set out in the US federal bank and thrift regulatory agencies' *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*. The banks take their responsibility to keep customers appropriately informed very seriously. We believe that organizations recognize their responsibility and have effectively been fulfilling that responsibility on a voluntary basis so that there is no need to legislate such a requirement. Any new enforcement mechanism would be inconsistent with the existing ombudsman model of the OPCC and may have a significant negative impact on both consumers and organizations.

In the U.S., where there are many state and federal laws requiring notification, consumers have become inured to hearing about breaches, experiencing "notification fatigue" with the result that they may pay less attention to notices when a serious breach has occurred and action is necessary. On the other hand, inappropriate breach notification can raise alarm needlessly, as occurred recently when the U.S. Department of Veterans Affairs advised of a breach and created the mistaken impression among large numbers of veterans that their personal information had been compromised, when in fact it had not.

The Privacy Commissioners of Canada, British Columbia and Ontario all support providing guidance for organizations to help them appropriately inform individuals of serious breaches, but they question whether mandatory breach notification is in the best interests of individuals or organizations. The Ontario and British Columbia commissioners have both published guidelines on breach notification, an approach that the banks would support at the federal level.

If, however, the Government deems it necessary to legislate notification requirements, it should be implemented as part of a fraud statute or as a separate statute dealing with identity theft and related issues so that these related measures can be dealt with in a coordinated and consistent way. We do not believe that the Act is the appropriate statute to deal with this issue.

## **Transborder Flows of Personal Information**

The banking industry believes that the current provisions in the Act provide sufficient protection for information that crosses international borders.

The Act requires that banks protect the personal information that they collect, and allows banks to outsource functions and provide personal information to those outsourcers as long as that personal information receives the same level of protection as provided by the bank (Schedule 1 of the Act, 4.1.3). Provisions that allow for the disclosure of information without consent for investigative purposes (subsections 7(3)(c.1),(c.2) and (d)) – an established element of privacy law in Canada that ensures effective investigations can occur – similarly apply to outsourcers used by banks. All provincial and federal public and private sector privacy statutes already permit disclosure of personal information for purposes relating to law enforcement.

The banks' outsourcing of functions is also governed by the Office of the Superintendent of Financial Institutions' *Guideline on Outsourcing of Business Activities, Functions and Processes*, available on OSFI's web site at [http://www.osfi-bsif.gc.ca/eng/documents/guidance/docs/b10\\_e.pdf](http://www.osfi-bsif.gc.ca/eng/documents/guidance/docs/b10_e.pdf). The Guideline sets out the bank's ultimate accountability for all outsourced activities and establishes guidelines and expectations for

financial institutions as they put in place processes for reducing the risks associated with outsourcing, and procedures to ensure adequate oversight of the outsourced activities.

As a general comment, the Canadian economy derives many benefits from outsourcing. Outsourcing of a variety of business processes is a reality of business operations, allowing organisations to cut costs and focus on core operations while providing customers with service, all in a highly competitive and cost conscious international environment. Business opportunities generated from US outsourcing contracts to Canadian firms create employment for Canadians, which generates tax revenue for governments, and ultimately contributes to Canada's economic growth and prosperity.

Outsourcing allows firms the scope and capability to deliver cost savings to customers. Outsourcing of administrative functions has become an established practice for many businesses. With an increased focus on accountability, businesses today must constantly make choices on how to provide their customers with services efficiently and for the best value.

Conflicts inevitably arise between the interest in maintaining the privacy of personal information, on the one hand, and the legitimate requirements of law enforcement, civil litigation and other types of legal process. Privacy legislation in Canada resolves such conflicts by permitting disclosures of personal information pursuant to legal process and for law enforcement purposes, subject to safeguards.

Governments around the globe have long exercised the right to obtain information held by organizations within their borders. Many Canadian laws also enable police, security agencies and government departments generally to obtain access to personal information held in Canada. In short, Canadian government agencies can obtain personal information held in Canada about foreign individuals, just as a foreign government can obtain personal information that may be held in that country about Canadians. Furthermore, Canadian police and security agencies can obtain information held abroad about foreign individuals by using mutual legal assistance procedures and information-sharing agreements.

Any contractual provisions that are considered to augment existing provisions in the Act should be voluntary.

## **Conclusion**

The Act has served Canadians well over the first four years of its operation, encouraging organizations to protect the personal information that they have about individuals and also encouraging individuals to be more aware of their rights and responsibilities to protect their own personal information. Nevertheless, as with any new legislation, there are some areas where experience with implementing the legislated requirements identifies areas where improvements would be desirable. We hope that this commentary assists the Committee with its review of the Act.