



# Submission by the Canadian Bankers Association to Industry Canada

Implementation of the Government of  
Canada's Response to the Fourth Report  
of the Standing Committee on Access to  
Information, Privacy and Ethics on the  
Personal Information Protection and  
Electronic Documents Act.

January 15, 2008



CANADIAN BANKERS ASSOCIATION

## Introduction

As part of its five-year review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the government responded to the recommendations made by the Parliamentary Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee), agreeing that generally PIPEDA is working well and setting out some minor adjustments to the legislation. The government's response provided a clear signal that it is committed to maintaining a strong, effective, and balanced approach to privacy protection in Canada.

The CBA was pleased to see the government's decision to create a definition of "business contact information" that would ensure that other business contact information, such as business e-mail and fax numbers, are exempt from the definition of personal information. It is important that both current and future technologies are captured in the exemptions so that business communication is not hampered.

We appreciate the government's intent to allow organizations to collect, use and disclose personal information as necessary for the conduct of business transactions, such as mergers and acquisitions and securitizations.

Allowing for the disclosure of personal information without consent in cases warranted by a strong individual, family and public interest is also a very positive change that our industry supports. It will allow banks, where they identify potential financial abuse, to take steps to seek assistance for customers at risk.

We are pleased to contribute the industry's views in response to the further government consultations announced in the *Canada Gazette Part I* on October 27, 2007. Our comments will focus on breach notification, a suggested alternative to the current process for the designation of investigative bodies, and financial abuse prevention measures. We also offer other suggestions for amendments that could help address certain operational issues with PIPEDA.

## Breach Notification

The banking industry supports the need to notify individuals of data breaches where an internal investigation concludes that there is a high risk of significant harm, including situations where personal information could be misused for fraudulent purposes or identity theft. We believe that this is the right thing to do to protect the individuals whose information we hold. We further believe that organizations in Canada recognize their responsibility and have been fulfilling that responsibility effectively on a voluntary basis, so there is no need to legislate breach notification requirements. Indeed, recently, the Privacy Commissioner engaged in a consultation process with various stakeholders to develop voluntary *Privacy Breach Guidelines* that build on an organization's obligation, already found in PIPEDA, to safeguard personal information.

We were pleased to see the government recognize that most Canadian organizations have been handling breach notification responsibly, and we encourage it to defer the adoption of a legislative framework and give the voluntary guidelines an opportunity to be fully adopted and tested by organizations of all sizes. Nonetheless, we are pleased to provide the banking industry's views on breach notification, should the government decide to proceed with a legislated requirement within PIPEDA.

The banking industry is of the view that, given the unique nature of each breach situation and the need for organizations to tailor their actions to the individual circumstances of the breach and varying levels of risk of harm, any legislated provisions should build in maximum flexibility for organizations to respond as appropriate. This would necessitate a principles-based approach whereby legislated provisions set out a broad requirement to notify; more detailed standards could be set out in regulations or guidelines. The Commissioner's voluntary *Privacy Breach Guidelines* set out steps that private sector organizations should follow when a privacy breach occurs, and should be used as the standard for any new measures that are developed. These guidelines provide an appropriate level of protection for consumers in the Canadian marketplace and good direction for any organization that experiences a breach.

The voluntary guidelines were based on guidelines previously published by privacy commissioners in British Columbia, Alberta and Ontario. They were developed in consultation with consumer and business groups, including the banking industry, to ensure that privacy breaches are dealt with in a manner that is effective across various types of organizations regardless of size or complexity, and protects affected individuals from the risks of fraud and identity theft. These same guidelines have recently been used as a model for voluntary notification standards in New Zealand. While the voluntary *Privacy Breach Guidelines* have been in place for only a short time, we understand that the Privacy Commissioner's office has already noticed an increase in communication since the Guidelines were posted from organizations about actions that they have taken on breaches that have been experienced. Clearly organizations are responding to the Commissioner's guidance in a positive manner.

The banks believe, further, that any legislated breach notification requirement must fit within the existing ombudsman model set out in PIPEDA. It is our view that the creation of an offence with penalties for failure to notify would fundamentally change the nature of this model and would potentially affect other roles of the federal Privacy Commissioner's office – mediation, education and audit, for example – and may require a reconsideration of the role of the Federal Court under PIPEDA. In particular, organizations do not currently have the right to appeal a Commissioner's decision to the Federal Court. The banking industry strongly believes that such a right would be required should an offence with penalties for failure to notify be created in PIPEDA.

The banks believe that the current ombudsman model allows organizations to work with the federal Privacy Commissioner's office on a collaborative basis to bring about enhanced compliance. The Privacy Commissioner already has powers such as audits, Commissioner-initiated complaints and other types of investigation, litigation and the ability to publicly identify organizations and/or to pursue legal remedies in the federal courts. These provide a powerful incentive to organizations to comply and the means to compel compliance, if required.

In the commercial context, an organization's reputation is the cornerstone of its success and, if ever seriously damaged, is difficult to recover and can sometimes be lost irrevocably. 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 has not been protected properly. In the banking industry, protection of personal information is critical and a baseline expectation of our customers. Thus the Commissioner's ability to publish the names of organizations that fail to notify provides a serious incentive for most organizations to comply.

Our further thoughts on some of the breach notification parameters are set out below.

## **Limiting Scope of Requirements**

The banking industry supports the broad definition of a breach set out in the federal Privacy Commissioner's voluntary *Privacy Breach Guidelines*, on the understanding that the threshold for notification is based on a risk assessment with consideration of both the risk of harm and the ability of individuals to take steps to mitigate harm. We nonetheless believe that a legislated breach notification regime would be more manageable for both organizations and the federal Privacy Commissioner if it specified which types of data breaches are outside the scope of the notification requirements. The banks believe that it is important to exclude from the application of the requirements certain types of debit or credit card frauds, or frauds committed against bank customers through the Internet – such as “phishing”. Obviously, organizations may still notify customers in these and other similar situations where there is unauthorized access to personal information, but would do so voluntarily for risk management purposes and as part of our commitment to consumer protection and good customer service. Organizations, however, should not be mandated through privacy legislation to provide such notice.

The banking industry supports the approach taken in the U.S. financial institution regulators' *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Interagency Guidance) (<http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf>), which was developed jointly by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corp. and Office of Thrift Supervision. This document limits notice to situations where the organization and its service providers are controlling the personal information at the time of the breach. Consequently, mandatory notification would not apply where information is directly disclosed by a customer to a third party, such as through a fraudulent web site or compromised debit or credit card terminal at point of sale.

## **Threshold for Notification**

### **Notice to Affected Individuals**

The standard for notification should be a serious, material breach where there is a high risk of significant harm, for example in the financial context where personal information could be used for fraudulent purposes or identity theft. This is also the standard set out in the U.S. Interagency Guidance.

Determining the seriousness of the risk of harm must be based on an objective assessment that considers the sensitivity of the information, the extent to which it can potentially be misused based on the data elements involved, including whether the sensitive data is encrypted, redacted, or otherwise shielded from access, as well as the ability of individuals to take steps to mitigate harm. A one-size-fits-all approach should be avoided in favour of allowing organizations to determine whether consumers should be notified based on the particular risk factors involved in each data breach case.

The banking industry does not support a blanket exemption from notification for breaches involving encrypted information, because there are many levels of encryption, some of which do not effectively protect customer information. Banks believe that other possible exclusions, such as publicly available information or, in the

financial context, account numbers for closed accounts or accounts from which withdrawals or transfers are not possible (e.g., mortgage loan account numbers) are properly addressed in the context of an objective assessment that considers the sensitivity of the information, and do not require blanket exemptions from notification.

### **Notice to Privacy Commissioner**

Consideration should be given to a discretionary approach that allows organizations to determine whether to notify the federal Privacy Commissioner based on the magnitude of the data breach, as part of the risk test that must be applied when notifying customers affected by the breach. Our preferred approach would be to adopt the same standard for notifying the Commissioner and customers as outlined in the Commissioner's voluntary *Privacy Breach Guidelines*. This would entail notification to customers for data breaches where there is a "high risk of significant harm" regardless of number of impacted customers, and additional notification to the Privacy Commissioner of any of those data breaches considered "material" (i.e., those involving a significant number of customers). This approach encourage organizations to notify the Commissioner so that her office is prepared to respond to any public queries, is aware of the actions being taken to address the cause of the breach and its effects, and can provide any needed advice on request or retrospectively.

We would note in this regard that there may be situations that do not meet the standard of a "high risk of significant harm to individuals," where organizations nonetheless choose to provide notice on a voluntary basis for customer service or other reasons. Such voluntary notifications should not trigger a requirement to also notify the Commissioner.

Any regime for reporting to the Commissioner should be carefully crafted to balance the desire to track data on breaches with the need to avoid disincentives to providing notice to customers or reporting to the Commissioner. Thresholds set too low may both overburden the Commissioner's office and provide a disincentive for organizations to notify and report. For example, we do not believe there is any value to either the Commissioner or the public generally in requiring organizations to report non-material breaches such as isolated incidents involving small numbers of affected customers. It should also be made clear what the Commissioner will do with this information, assuming appropriate steps to manage the incident and assess risks have been taken and the notification process has been respected.

Further, there should be built into the reporting process some controls on how, when and by whom information should be shared publicly. An announcement made prematurely could interfere with the investigation of a breach or may cause unnecessary angst by even unaffected individuals. To this end, the additional requirement for organizations to report "any major loss or theft of personal information" to the Commissioner should be limited to situations where an organization concludes that the incident poses a high risk of significant harm to a significant number of its customers, or concludes that significant harm to customers has occurred. We believe that notice to the Commissioner prior to an organization having assessed the nature and scope of the incident and determined the likelihood, if any, that the information has been or will be misused is unduly burdensome for the Commissioner and organizations alike.

## **Timing of Notification**

Many U.S. states have enacted measures requiring organizations to notify individuals as soon as reasonably possible or “without unreasonable delay” following discovery of a breach. The Commissioner’s voluntary guidelines follow a similar approach by encouraging organizations to provide notice to individuals “as soon as reasonably possible following assessment and evaluation of the breach.” The banking industry supports these formulations to allow investigations to be undertaken to determine whether a breach has in fact taken place and, if so, the magnitude and impact of the breach and whether individuals should be notified. Imposing any specific standard of time would be arbitrary and inconsistent with the objective of allowing organizations to carry out their own due diligence and make assessments on a case-by-case basis. Clearly, an announcement made prematurely (e.g., prior to confirmation of breach, prior to confirmation of which individuals are impacted, or prior to set up of supporting communications such as call centre support) could cause unnecessary angst by the public, including individuals unaffected by the breach. This more flexible wording would also allow organizations to factor in requirements of law enforcement authorities who may delay notification to further their investigation and identification of the perpetrators of the breach.

As noted above, the industry’s preferred approach is notification to the Commissioner following completion of an internal assessment and evaluation of the breach, and at least concurrently with notification to individuals. The banks were pleased to see the government’s recognition that organizations are best placed to manage and assess risks associated with breaches, and we agree with its recommendation that the Commissioner should not be burdened with the responsibility to decide on notification. Of course, organizations may choose to consult with the Privacy Commissioner’s office at any point after they become aware of an incident, which may be particularly useful to smaller businesses that may lack the experience or internal resources to make risk assessments.

## **Manner of Notification**

U.S. state laws and the Commissioner’s voluntary guidelines also set out similar rules for the manner in which organizations should attempt to notify individuals. In both cases, notification to affected individuals should be direct – by phone, letter, email or in person. Indirect notification is allowed where direct notification could cause further harm, is prohibitive in cost, or the contact information for affected individuals is unknown. We believe that these criteria provide a fair, flexible, and effective way of ensuring individuals who are affected by a breach receive proper notice, and are consistent with the “reasonableness” standard set out in PIPEDA generally. Our review of published findings from provincial privacy commissioners, including Ontario where breach notification is mandated under *The Personal Health Information Protection Act*, leads us to believe that these offices have insights into the manner of notification and the need for flexibility that may be valuable in the context of the government’s consultations.

The banks believe that e-mail notification should only be permitted through secure channels where appropriate authentication and privacy protections have been adopted, and where the affected individual has consented to receiving important information in this electronic form.

The CBA also supports requirements that parallel the Commissioner's voluntary guidelines in terms of prescribing the type of information that must be disclosed to individuals. The voluntary guidelines focus on information that is of value to the individual, such as appropriate information about the incident and its timing in general terms; a description of the personal information involved in the breach, a general account of what the organization has done to control or reduce the harm, what the organization will do to assist individuals, and what steps the individual can take to avoid or reduce the risk of harm. Individuals receiving the notification want to know that the organization has taken its own steps to mitigate risk of harm and what else, if anything, needs to be done by them to further mitigate harm. Too much specific information about the breach may not be relevant or productive in helping the client manage their risk – it may instead result in a higher level of anxiety than warranted.

## **Notifying Credit Bureaus**

In situations where a breach creates a serious risk of harm to our customers, banks currently notify the affected individuals and instruct them to contact the credit bureaus to report the incident and discuss options for protecting themselves, such as including a credit alert on their report. In the case of security breaches where a large number of customers are potentially affected, banks will advise the credit bureaus to expect a higher volume of calls. Banks do not provide the credit bureaus with a list of the names of affected individuals. We are strongly of the view that affected individuals are in a better position to decide what measures are most appropriate for their own circumstances. Individuals are also the only ones able to provide all the information that a credit bureau would require to register an alert or implement any other preventative measures.

Any new statutory requirements should only compel organizations to provide their customers with information about the options available to them and to alert credit bureaus about the occurrence of a breach where a large volume of individuals are affected. In states such as Colorado, Michigan, New Hampshire, North Carolina and Pennsylvania, breach notification laws require bureaus to be advised about the occurrence of a breach when more than 1,000 individuals are affected. While there is merit to providing notice to bureaus in such circumstances, banks do not support any measure related to breach notification that requires organizations to share personal information of customers with credit reporting agencies.

## **Notifying Other Organizations**

The government has proposed consideration of a requirement for organizations experiencing a breach to notify other organizations that may be impacted by the breach. The example cited was a retailer experiencing a breach of customer credit card information should be required to notify the card issuers. The banks are strongly of the view that it is not necessary to include such a provision. The business relationship between organizations is a matter of contract and well covered in that context.

## **Prevention of Fraud and Investigative Bodies**

PIPEDA should be amended to follow the approach of the British Columbia *Personal Information Protection Act* (BC PIPA) 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.

In addition to the increased administrative burden on the government, the rapid expansion of the number of investigative bodies has resulted in an almost impossible task of determining who the members of these bodies are before an organization can be certain that it is acting appropriately by releasing information to these bodies. These challenges would be relieved if the government were to adopt language similar to the BC PIPA.

There are inconsistencies between the exemptions for collection, use and disclosure in PIPEDA 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 PIPEDA's inconsistencies among sections 7(1), 7(2) and 7(3). For instance, while PIPEDA 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. A bank is then permitted to 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.

Another problem area experienced by bank financial groups is that the membership in the BCPIO is restricted to certain bank employees and does not allow membership of staff in fraud or investigative units in other areas of the bank financial group. These excluded employees are integral to the fraud prevention and investigation functions of the financial group and should be able to be part of the larger group with access to the shared information.

The BC PIPA includes "prevention of fraud" as one of the acceptable components in its definition of "investigation" (s. 1 Definitions). While PIPEDA currently does not define "investigation", perhaps this concept could usefully be applied to provide greater ability to organizations to assist with the prevention of fraud and other contraventions of the law, such as money laundering, terrorist financing, etc.

In PIPEDA, "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 PIPA (s. 1) and AB PIPA (s. 1(f)) 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 PIPA).

We would recommend that PIPEDA 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.

## **Preventing Financial Abuse**

The CBA has noted in previous submissions that elder financial abuse is a significant issue in Canada. Data from Statistics Canada shows that approximately seven per cent of seniors have experienced some form of financial abuse and manipulation by an adult child, caregiver or spouse to misappropriate funds from the customer’s bank account. Bankers feel a moral obligation and are frequently under pressure from public interest groups and public authorities to act on their suspicion of financial abuse, with both elderly and other customers, and to report the suspected abuse to another family member or the authorities. Yet s. 7(3) of PIPEDA does not allow such disclosures without the customer’s consent, which is difficult to request in this type of situation.

We appreciate the government’s stated intent to amend PIPEDA so that elder abuse can be addressed. Guidance may be available in the BC PIPA and the Alberta *Personal Information Protection Act* (AB PIPA) that define “legal proceeding” to include remedies “claimed ... under the common law or in equity”, or “available at law”, both of which would allow the banks to use the common law duty under the *Tournier v National Provincial & Union Bank of England (1924)* decision to help avoid financial abuse.

## **Other Issues**

### **Debt Collection**

Section 14(i) of AB PIPA allows an organization to collect personal information without consent if the information is necessary to collect a debt owed to the organization. This exception to consent for collection is consistent with AB PIPA’s exception to consent for disclosure for debt collection. A similar exception for collection specific to debt collection does not currently exist in PIPEDA and would provide greater certainty for banks regarding the practices that must be followed for debt collection. This would include clarifying a bank’s ability to collect information about a debtor’s current address and the ability of banks to record customers’ calls in these circumstances. Although s. 7(3)(b) of PIPEDA allows for *disclosure* without consent for the purpose of collecting a debt, thereby recognizing that debt collection might be jeopardized if consent is required, there is no similar provision for *collection* without consent. The inadvertent result of this is a higher bar for collection than for disclosure, which surely is an unintended effect. Banks need to be able to collect information without consent for debt collection. Where a defaulting debtor has moved, the new address needs to be obtained so the bank can contact the debtor. Similarly, an exception would be necessary when a collection call is being recorded. If the defaulting debtor is able to refuse consent for the taping of the call, it would either cause the call to end before collection can be discussed or preclude the bank from recording evidence of the debtor’s commitment to pay. Accordingly, the CBA recommends that the circumstances in PIPEDA for collecting personal information without consent be expanded to more closely align with the circumstances found in Alberta’s PIPA to facilitate banks’ debt collection practices.

## **Commissioner's Authority to Dismiss Unsupported Complaints**

Since PIPEDA came into force in 2001, it has become evident that the Privacy Commissioner's Office receives many complaints that are only tangentially related to privacy (e.g., isolated disputes between estranged spouses where an individual's personal information has been used to gain access to their financial accounts). Such cases do may not merit the resources required to conduct investigations by either the Privacy Commissioner's office or the affected organization. To reduce the number of unnecessary investigations for both parties and to improve the Office's ability to respond to legitimate complaints, to allow it to focus on more important systemic issues and to achieve more efficient case management, the banking industry supports providing the Commissioner with greater flexibility to dismiss disputes that are clearly not in the public interest. As currently enacted, PIPEDA requires the Commissioner to conduct an investigation in respect of all complaints it receives, with the only discretion being whether a report must be prepared. There is no ability to assess the validity of complaints and avoid expending resources on unnecessary investigations.

The Alberta Select Special *Personal Information Protection Act* Review Committee has recently studied this issue in its three-year review of that province's privacy framework. In recommendation 32 of its final report (<http://www.pipareview.assembly.ab.ca/report/finalpipawReport111407.pdf>), the Committee recommended that PIPA be amended to provide the Commissioner with explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed. The banking industry recommends that the federal Commissioner also be provided explicit authority in this regard so that the Commissioner may decide not to commence an investigation or not to continue an investigation already begun where it is found that the complaint is without merit.

## **Conclusion**

In closing, we appreciate the opportunity to be a part of the process to enhance and modernize the standards governing the protection of personal information in the private sector. We would ask that you take into consideration the issues and suggestions we have raised to help create an effective regulatory framework that will serve all Canadians for years to come.