GILLMAN & GILLMAN
Barristers & Solicitors

Volume 1
No. 4
Fall, 2005

The Financial Services Regulatory Report

Ontario *Consumer Protection Act, 2002* – Some Implications for Financial Institutions

The new *Ontario Consumer Protection Act, 2002* together with Ontario *Regulation 17/05* (collectively the "CPA") which came into force on July 30, 2005 dramatically expand the rights of consumers in Ontario. Companies located in Ontario, or which sell, lease or finance products or services to consumers located in Ontario are now subject to a broad range of new obligations and will have to revise their contracts and business practices to meet this far-reaching new legislation.

Credit Card Disclosure Requirements

The legislation will significantly affect provincially regulated credit card issuers, including credit unions and other financial institutions incorporated provincially and other non-financial institutions which issues credit cards.

However, as the field of cost of borrowing disclosure insofar as it affects direct loans by banks to their customer has been fully "occupied" by the federal *Bank Act* and the *Cost of Borrowing (Banks) Regulations*, the provincial CPA's disclosure requirements are considered inoperative as they relate to banks.

Other federally regulated financial institutions may be affected to the extent that gaps exist between legislative requirements imposed at the federal and provincial levels.

The CPA brings the federal/provincial agreement for harmonization of cost of credit disclosure laws into Ontario. In particular, the CPA:

- ✓ establishes new cost of credit disclosure rules;
- ✓ prohibits credit card issuers from imposing default charges other than certain prescribed charges incurred by the issuer;
- ✓ contains certain limitations and restrictions relating to charges for optional services;
- ✓ establishes cardholder's maximum liability for unauthorized charges;
- ✓ establishes disclosure requirements where the credit card issuer invites the cardholder to defer payments otherwise due;
- ✓ establishes rules regarding unsolicited credit cards;
- ✓ establishes rules regarding credit card advertising.

Internet Agreements

The CPA also imposes new obligations on suppliers and gives new rights to consumers who conduct business on the Internet. The new regime applies to consumer agreements that involve payments of more than $50 and to suppliers *or* consumers who are located in Ontario when the transaction takes place.

The following are some of the principal new obligations and rights under the CPA regarding Internet agreements:

- ***Disclosure***
  Suppliers are required to make disclosure of specified information in a way that is clear, comprehensible and prominent and that allows the consumer to print the information. This disclosure includes, amongst others, the following information:
  - ✓ A fair and accurate description of the goods and services;
  - ✓ Amount and frequency of payments;
  - ✓ The date, location and manner of delivery or performance;
  - ✓ If the supplier holds out that another person would provide the services on the supplier's behalf, the name of that person;
  - ✓ The rights of cancellation, return, exchanges, refunds and trade-ins;
  - ✓ Other "restrictions, limitations and conditions" imposed by the supplier.
- ***Acceptance***
  Suppliers must provide consumers with an express opportunity to accept or decline the Internet agreement and to correct errors immediately before entering into it.
- ***Terms of the Agreement***
  Provisions in an Internet agreement that require resolution by arbitration or that limit the right of the consumer to resolve disputes in court will not be enforceable. In addition, any ambiguities in an Internet agreement will be resolved in favour of the consumer.
- ***Delivery***
  A written copy of the Internet agreement must be delivered (e.g. by fax, e-mail, mail or courier) to the consumer within 15 days of entering into the agreement. The Internet agreement must include the disclosures indicated above as well as the name of the consumer and the date the agreement was entered into.
- ***Cancellation Rights***
  A consumer may cancel the agreement at any time after the agreement was entered into until 7 days after receiving a copy of it *if* the supplier failed to disclose the specified information or give the consumer an opportunity to accept, decline or correct the agreement. The consumer has a further right of cancellation within 30 days of the date the agreement was entered into *if* the supplier does not provide a copy of the Internet agreement to the consumer.
- ***Amendment, Renewal and Extension by the Supplier***
  The CPA severely restricts the ability of suppliers to unilaterally amend, renew or extend consumer agreements including Internet agreements.

Recent Privacy Developments

Bank's notification to customers triggers PATRIOT Act concerns

Several customers of a Canadian chartered bank complained to the Office of the Privacy Commissioner (OPC) after the bank sent a notice to its customers amending its credit cardholder agreement. The amendment advised of the use of a service provider located in the United States and of the possibility that U.S. law enforcement or regulatory authorities might obtain access to customer's personal information under the U.S. *Patriot Act*.

Customers filing the complaints alleged that:

- The bank required its credit card customers to consent to the disclosure and use of their personal information to U.S. regulatory authorities as a condition of service;
- Customers were being required to consent to overly broad collection practices;
- The bank would not allow them to opt-out of having their personal information sent to the third-party service provider; and
- The bank was not properly safeguarding their personal information.

On October 19, 2005, the Assistant Privacy Commissioner released her finding that the complaints were ***not well-founded***. She concluded as follows:

- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not prohibit the use of foreign-based third-party service providers; it does oblige Canadian-based organizations to have provisions in place, when outsourcing to third-party service providers, to ensure a comparable level of protection.
- In keeping with its obligations under Principle 4.1.3 of PIPEDA and in accordance with the Office of the Superintendent of Financial Institution's (OSFI) guidelines (which she found to be consistent with this Principle), the bank's contract with its third-party service provider provided guarantees of confidentiality and security of personal information.
- The Assistant Commissioner noted, however, that while a customer's personal information is in the hands of a foreign third-party service provider, it is subject to the laws of that country and no contract or contractual provision can override those laws. In short, an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its customers' personal information from being lawfully accessed by U.S. authorities.
- It was clear to the Assistant Commissioner that there is a comparable legal risk that the personal information of Canadians held by any organization and its service provider — be it Canadian or American — can be obtained by government agencies, whether through the provisions of U.S. law or Canadian law.
- The Assistant Commissioner reaffirmed the OPC's position that, at the very least, a company in Canada that outsources information processing to the United States should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country. In fact, the bank had informed its customers of the *risk* that their personal information could be lawfully accessed by U.S. authorities.
- The Assistant Commissioner further reaffirmed its position that companies are not required to provide customers with the choice of opting-out where the third-party service provider provides services directly related to the primary purposes for which the personal information was collected.
- However, the Assistant Commissioner decided that the cardholder agreement was unclear in that it left the impression that customers could opt-out of disclosure of their personal information to the third-party service provider. This contradicted the language of the bank's privacy policy. As a result, the Assistant Commissioner suggested that the bank review and amend its cardholder agreement to provide greater clarity on this point.

Opting out of Marketing Inserts in Bank Statements

A customer complained to the federal Privacy Commissioner when his bank refused to allow him to opt out of receiving marketing materials inserted with his credit card statement.

The bank contended that the inserts were not addressed personally to the customer but were placed, without distinction, in the account statements addressed to all credit card customers. In the bank's view, this did not constitute a "use" of the customer's personal information. In addition, the bank informed customers through its account agreement and disclosure statements that they might receive marketing information with their account statements. The bank did not consider inserts to be a form of secondary marketing in the same way telephone or other direct marketing might be and from which the customer might opt-out.

The Assistant Privacy Commissioner, however, found the complaint to be "well-founded" and concluded as follows:

- As the goal of placing inserts in the same envelope as the account statements was nevertheless one of marketing, the result was a *use* of the customer's information.
- The insertion of marketing material in a statement of account was secondary to the primary purpose for which the customer initially provided the information to the bank, i.e., for the purposes of determining creditworthiness, issuing a credit card and administering the account.
- By not providing a means of withdrawing consent to this form of secondary marketing, the bank was requiring the customer to consent to a use of his personal information beyond that required to service his credit card account, in contravention of Principles 4.3.3 and 4.3.8 of Schedule I of the federal *Personal Information Protection and Electronic Documents Act.*

OSFI's Review of Reputational Risk Practices: Principles, Observations and Next Steps

In June, 2005, the Office of the Superintendent of Financial Institutions ("OSFI") issued a *Review of Reputation Risk Practices: Principles, Observations and Next Steps.* The document communicates basic principles associated with reputation risk management, highlights observations from OSFI's work in this area and discloses issues that OSFI might raise during supervisory reviews.

OSFI is of the view that improving the effectiveness of reputation risk management practices should be a priority for all financial institutions. As a result, OSFI will pay increasing attention to how financial institutions are managing reputation risk. Each financial institution should adopt an approach to reputation risk management that takes into account the nature, scope, complexity, and risk profile of the institution.

OSFI is of the view that the following activities are important for effective reputation risk management:

- Senior management and boards should be actively involved with the development and implementation of effective reputation risk management practices. During future supervisory assessments of financial institutions and depending on its scope and complexity of operations, OSFI may query whether senior management and the board have assigned appropriate roles and responsibilities for reputation risk management practices and whether, generally speaking, the board has communicated a strong commitment to protecting the bank's reputation.
- Financial institutions should have effective policies that establish a framework for managing reputation risk on an on-going basis. During future supervisory reviews, OSFI may focus on whether appropriate *written policies* have been adopted, whether they adequately address all facets of effective risk management practices and if they are understood by the organization and followed.
- Financial institutions should have procedures to monitor the effectiveness of reputation risk management practices, regular reporting to senior management and the board and ensuring appropriate actions are taken when required. Future supervisory assessments will focus on how reputation risk management practices are being monitored, the quality and timeliness of reports and the extent to which issues are analysed and addressed.
- Financial institutions should ensure that all employees are aware of and capable of identifying and managing reputation risks within their areas of responsibility. Future supervisory assessments will focus on the nature of *training* provided to employees, who receives training and how often and whether there is follow up to ensure the training is relevant.
- Financial institutions should ensure their practices for controlling reputation risk are reviewed by their internal audit group. In future supervisory reviews, OSFI may inquire whether internal audit has reviewed the level of adherence to reputation risk management practices.

Final OSFI Administrative Monetary Penalties Regulations

The *Administrative Monetary Penalties (OSFI) Regulations* (the "Regulations") received final approval on August 30 2005 and are published in the September 21, 2005 issue of the Canada Gazette Part II (SOR No.267). The Regulations implement an administrative monetary penalties regime under which the Superintendent can impose penalties for specific violations by federally regulated financial institutions, as designated in the schedule to the Regulations. The Regulations replace the current *Filing Penalties (OSFI) Regulations*, which came into force on April 1, 2002.

The main objective of the Regulations is to designate the specific violations of the federal financial institutions statutes for which OSFI can impose a penalty. Each contravention is classified as "minor", "serious" or "very serious". In general, late and erroneous filing contraventions are classified as minor, while contraventions that impact on the safety and soundness of the financial institution are classified as serious or very serious.

The monetary penalties imposed vary depending on how the contravention is classified. Subject to the maximum amounts set out in section 25(2) of the *OSFI Act*, the Superintendent has discretion to fix the amount of the penalty using the criteria set out in section 26 of that Act. For late or erroneous filing contraventions, however, the amount of the penalty is a function of the size of the institution in terms of assets and the number of days that the contravention occurs to the maximum set out in the Regulations.

The *Administrative Monetary Penalties* framework applies to banks and federally regulated insurance companies, loan and trust companies, and entities governed by the federal *Cooperative Credit Associations Act.*

Canadian Payments Association Publishes a Guide to Risk in Payment Systems

In July, 2005, the Canadian Payments Association issued "*A Guide to Risk in Payment Systems Owned and Operated by the CPA*". The purpose of the paper is described as follows:

- to define, identify and generally explain the risks associated with using or participating in the Canadian Payments Association-owned or operated systems;
- to illustrate the risk scenarios within the payments system and suggesting methods to manage and mitigate such risks; and
- to encourage financial institutions who participate in the Canadian Payments Association's payment systems to implement risk management systems within their own financial institutions.

A full copy of the CPA publication is available at:
http://www.cdnpay.ca/news/pdfs_news/Risk%20Guide.pdf

If you require assistance on how any of the above-noted matters will affect your organization, please call Libby Gillman at 416.418.7204 or contact her at libbyg@lawgill.com

The Financial Services Regulatory Report is published periodically to keep you informed of developments in financial services legal and regulatory matters. This Report is a general discussion of certain legal developments and should not be relied upon as legal advice. If you require legal advice or financial regulatory consulting services, we would be pleased to discuss with you the issues raised in this Report in the context of your particular circumstances.