GILLMAN & GILLMAN
Barristers & Solicitors

Volume 6
No. 1
Summer/Fall, 2010

The Financial Services Regulatory Report

Minister of Finance Announces Task Force to Review Payments System

On June 18, 2010 (the second day of the Canadian Payments Association's "Payments Panorama 2010" conference, held in Vancouver), The Honourable Jim Flaherty, Minister of Finance, announced the launch of the Task Force for the Payments System Review. The announced purpose: to help guide the evolution of the payments system in Canada.

The mandate of the Task Force is to review the safety, soundness and efficiency of the payments system; to assess if there is sufficient innovation in the payments system; consider the competitive landscape; decide whether businesses and consumers are being well served by payments system providers; and determine whether current oversight mechanisms for the payments system remain appropriate.

The Task Force must provide the Minister of Finance with its recommendations by the end of 2011. In the coming weeks, the task force will invite submissions from stakeholders and all interested Canadians.

*The recommendations of the Task Force will be heavily influenced by the input it receives from stakeholders. Should you need assistance in developing your submission to the Task Force**, please contact Libby Gillman of Gillman Professional Corporation, Barristers & Solicitors at 416.418.7204 or at libbyg@lawgill.com.***

Voluntary Code of Conduct for Credit and Debit Card Industry in Canada

On May 18, 2010, the Minister of Finance also announced that all payment card networks, major credit and debit card issuers and payment processors have adopted the *Code of Conduct for the Credit and Debit Card Industry in Canada* (**"**Code").

Under the Code, payment card networks and their participants must ensure increased transparency and disclosure to merchants including ensuring that merchant-acquirer agreements and monthly statements contain a sufficient level of detail and are easy to understand. Payment card networks must also make all applicable interchange rates easily available on their websites.

In addition, payment card network rules must ensure that:

1. merchant statements include the following information:

    a. Effective merchant discount rate for each type of payment card from a payment card network;

    b. Interchange rates and, if applicable, all other rates charged to the merchants by the acquirer;

    c. The number and volume of transactions for each type of payment transaction;

d. The total amount of fees applicable to each rate; and

e. Details of each fee and to which payment card network they relate.

This information must be presented in a manner that is clear, simple and not misleading.

2. merchants will receive a minimum of 90 days notice of any fee increases or the introduction of a new fee related to any credit or debit card transaction. Payment card networks must also provide at least 90 days notice to acquirers for rate and/or fee changes and at least 180 days notice for structural changes;

3. following notification of a fee increase or the introduction of a new fee, merchants may cancel their contracts without penalty;

4. merchants who accept credit card payments from a particular network cannot be compelled to accept debit card payments from that same payment card network, and *vice versa*;

5. merchants will be allowed to provide discounts for different methods of payment (e.g., cash, debit card, credit card). Merchants must also be allowed to provide differential discounts among different payment card networks;

6. competing domestic applications from different networks must not be offered on the same debit card. However, non-competing complementary domestic applications from different networks may exist on the same debit card;

7. co-badged debit cards are equally branded;

8. debit and credit card functions shall not co-reside on the same payment card;

9. premium credit and debit cards are only given to consumers who apply for, or consent to receive, such cards. In addition, premium payment cards shall only be given to a well-defined class of cardholders based on individual spending and/or income thresholds and not on the average of an issuer's portfolio; and

10. negative option acceptance by merchants of new products and services is not allowed.

Most elements of the finalized Code will be effective starting August 16, 2010.

Once passed, Part 12 of Bill C-9, the *Jobs and Economic Growth Act* will enact the *Payment Card Networks Act* to regulate national payment card networks and the commercial practices of payment card network operators. This Part also makes related amendments to the *Financial Consumer Agency of Canada Act* to expand the mandate of the Agency to supervise payment card network operators and their compliance with the Code.

Government of Canada Moves to Enhance the Personal Information Protection and Electronic Documents Act

On May 25, 2010, the Government of Canada introduced amendments to the legislation protecting the personal information of Canadians in a Bill entitled *An Act to amend the Personal Information Protection and Electronic Documents Act* (PIPEDA).

The bill makes some important changes, including creating exceptions to the consent requirement for business contact information and work product information and requiring mandatory breach reporting. Details of the key changes are set out below.

Consent Requirement for Business Contact Information

Pursuant to the proposed amendments, business contact information collected, used or disclosed solely for the purpose of communicating with the individual in relation to their work, would be excluded from the requirements of PIPEDA.

"Business Contact Information" means an individual's name, position name or title, work contact details (including e-mail address) and any similar information of the individual.

Mandatory Breach Notification

To address public concerns about the increasing number of data breaches involving personal information, the bill sets out a new requirement for organizations to report *material* data breaches to the Privacy Commissioner of Canada and to notify individuals when there is a real risk of significant harm to the individual, such as bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. The materiality of the breach would be assessed based on criteria that include sensitivity of the personal information, the number of individuals affected and whether the breach is indicative of a systematic failure of security.

The notice must contain sufficient information to allow individuals to understand the significance of the breach to them and to take steps to mitigate that harm. Notice has to be given as soon as feasible after the organization confirms the occurrence of the breach and concludes that it is required to give the notice. The form and manner of notice will be set out in regulations.

The breach notification requirement will complement the government's recently enacted identity theft legislation and encourage better information security practices on the part of organizations.

Business Transactions

Proposed amendments to PIPEDA would permit organizations that are parties to a "prospective business transaction" to use and disclose personal information without the knowledge or consent of the individual if they have entered into an agreement that requires the recipient (i) to use the information and disclose it solely for the purposes related to the transaction, (ii) to protect that information with appropriate safeguards and, (iii)if the transaction does not proceed, to return or destroy the information within a reasonable period of time. As well, the personal information must be necessary to determine whether to proceed with the transaction and to complete the transaction. A "business transaction" is defined to mean a range of transactions, including purchase or sale of a business, mergers and amalgamations, financings, lease or licensing of the organization's assets, and joint ventures.

Once the transaction is completed, the parties to the transaction may use and disclose the personal information without consent, provided:

(1) they have entered into an agreement that requires them to (i) use and disclose the personal information solely for the purpose for which it was collected or permitted to be used or disclosed before the transaction was completed (ii) protect the information by security safeguards commensurate with the sensitivity of the information and (iii) give effect to any withdrawal of consent made in accordance with Principle 3 of Schedule I;

(2) the personal information must be necessary for carrying on the business or the activity that was the object of the transaction; and

(3) the individual is notified within a reasonable time after the transaction has completed of the transaction and that their personal information has been disclosed.

Other Amendments

Other key amendments:

- clarify that the consent that is required under PIPEDA is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

- purport to clarify the meaning of "lawful authority" for purposes of disclosing information to government institutions and law enforcement without knowledge or consent of the individual. These changes provide that lawful authority refers to lawful authority *other than* a subpoena, warrant, or court order or rules of court relating to production of records. They also provide that the organization that discloses personal information is not required to verify the lawful authority identified by the government institution.

- remove the concept of investigative bodies. Instead, the amendments would permit disclosure to another organization where that disclosure is necessary to investigate a breach of an agreement or a violation of the laws of Canada or of a province or is necessary to prevent, detect or suppress fraud where it is reasonable to expect the disclosure with the knowledge or consent of the individual would undermine the ability to prevent, detect or suppress the fraud.

In addition, the bill re-introduces anti-spam legislation (the proposed *Fighting Internet and Wireless Spam Act*, or FISA).The proposed FISA is intended to deter the most damaging and deceptive forms of spam, such as identity theft, phishing and spyware, from occurring in Canada and to help drive spammers out of Canada.

The proposed FISA legislation provides a comprehensive regulatory regime that relies on economic disincentives to protect electronic commerce and is modelled on international best practices.

To enforce the legislation, the bill would use the expertise, and expand the mandates, of the following three enforcement agencies: the Canadian Radio-Television and Telecommunications Commission, the Competition Bureau Canada and the Office of the Privacy Commissioner of Canada.

Competition Bureau Announces Decision in Response to Interac's Request to Vary Consent Order

Earlier this year, the federal Competition Bureau turned down a request by Interac Association to allow the debit payment processor to become a for-profit business.

Interac is governed by a consent order issued some years ago by the Competition Tribunal intended to prevent the company from engaging in anti-competitive practices which would substantially lessen competition. Interac's desire to restructure from a not-for-profit association structure to a for-profit model would require a change to that order.

In rejecting Interac's request, the Bureau suggested that Interac could change its mode of operations, including to its governance structure, in a way that would allow it to remain competitive to new challenges in the market, while maintaining its non-profit status.

While the Bureau would not support an application to vary the Consent Order to permit for–profit activities by Interac at this time, the Commissioner indicated the Bureau would

re–examine Interac's request if there is new information, material changes occur in the marketplace, or if Interac advances an alternative proposal, provided that any changes approved would not impact the key elements of the current Consent Order.

CPA Payments Strategy: Vision 2020

In 2008, the Canadian Payments Association ("CPA") embarked upon a comprehensive exercise to develop a strategy to ensure that its framework for clearing and settlement serves the needs of all participants and the Canadian public.

Following the public release of a draft of its Vision 2020, CPA embarked, in 2009, upon an extensive consultation program to engage a wide variety of participants including corporate stakeholders, payment service providers, consumer organizations, member financial institutions, and other interested parties.

The feedback collected during the 2009 consultation helped to shape the final strategy into a CPA roadmap for personal, corporate and wholesale payments over the next decade.

Pursuant to CPA's Payment Strategy: Vision 2020, the CPA will:

- Support the Growth of Electronic Payments
- Drive Efficiencies in Payments
- Modernize the CPA Regulatory Framework & Rules
- Enhance Exchange, Clearing and Settlement Systems
- Expand Value-added Services

The full text of the CPA's Vision 2020 is available at
http://www.cdnpay.ca/news/pdfs_news/payments_strategy_vision_2020.pdf

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.