GILLMAN & GILLMAN
Barristers & Solicitors

Volume 7
No. 1
Summer/Fall,
2012

The Financial Services Regulatory Report

Update on the Canadian Task Force for the Payments System Review

On June 18, 2010, the Honourable Jim Flaherty, Minister of Finance, announced the launch of the Task Force for the Payments System Review ("Task Force"). The announced purpose: to help guide the evolution of the payments system in Canada.

The mandate of the Task Force was 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 conducted two online consultations, regional roundtables and a series of working group meetings to promote dialogue and cooperation within the payments industry. It drew stakeholders from a wide range of sectors, including federal and provincial governments, consumer groups, non-financial businesses and the financial sector.

The Task Force Report

On March 23, 2012, the Minister of Finance released "*Moving Canada into the Digital Age",* the final report of the Task Force for the Payments System Review.

The Task force concluded that unless Canada develops a modern digital payments system, Canadians will be unable to engage fully in the rapidly evolving digital economy of the 21st century, leading to a lower standard of living across the country and a loss in international competitiveness. The Task Force stated that while Canadians have a tendency to be early adopters of technology, Canadians still rely on outdated methods of payment such as paper-based processing and cash and cheques. In addition, Canada is falling behind in the international push to generate a secure mobile ecosystem. The Task Force further concluded that the Canadian payment system is outdated because it is dominated by the major banks and other key institutions whose interests are best served by keeping at bay new entrants into the payments system.

To remedy Canada's outdated payment system, the Task Force recommended that the Government of Canada needs to take the lead in several critical areas:

1. A feature-rich electronic invoicing and payments system for businesses.
2. A state of the art mobile payments system for consumers.
3. A secure digital identification and authentication regime.
4. A governance structure to allow collaboration and innovation.

The Task Force also concluded that governments need to recognize payments as a bona fide and discrete industry. It settled on the following working definition of who should be considered to be a payment system provider:

"The payments system refers to arrangements that allow consumers, businesses, governments and other organizations to transfer monetary value from one party to another. It includes the institutions, instruments and services that facilitate the transfer of monetary value between parties in a transaction."

It further concluded that Government needs to formally enshrine high-level principles of trust, access and good value that serve the public interest. While the Task Force indicated that it favours "light-touch legislation" to protect the public interest, the Task Force recommended the creation of a public oversight body which would monitor how changes to the payment system are implemented and to ensure that those changes reflect the wants and needs of the Canadian public. The oversight body would report directly to the Minister of Finance but would delegate its regulatory and policy-making functions to a self-governing organization ("SGO") while retaining the right to ratify the strategies of the SGO and review its performance. All payments providers would be required to be members of the SGO and users would be eligible for membership. The oversight body would also provide recourse to stakeholders who could not resolve their concerns within the SGO.

The Task Force also proposed that Government undertake changes to the objects, governance, powers, business and funding model of the Canadian Payments Association to enable it to provide an infrastructure that underpins an innovative payments system for the future.

The Minister's Response

At the Canadian Payments Association's *Payments Panorama* conference held in Quebec City in June, 2012, the Minister announced the initiatives which the Government would be taking to respond to the Task Force's final report. The initiatives include:

- reviewing the governance framework for the payments system and establishing the Finance Canada Payments Consultative Committee ("FinPay") to help the Government stay abreast of market developments and to contribute to policy development in support of an innovative and safe payments system. The Minister stated that, "FINPAY will help the government stay current about market developments and will contribute to the elaboration of effective policy that supports an innovative and safe payments system that meets the needs of consumers and merchants." He further indicated that the Department of Finance is currently finalizing the terms of reference and membership of this committee, and that the first meeting will convene once that work has been completed.

- reviewing the Code of Conduct for the Credit and Debit Card Industry in order to respond to the evolution of mobile payments.

- taking a "fresh look" at how the Canadian payments system and its participants are governed to ensure continued safety and soundness of the system, while spurring innovation and promoting consideration of user interest.

Establishing Canada as a Centre of Excellence for Mobile Payments: the Canadian NFC Mobile Payments Reference Model

The Task Force asked Canadian financial institutions to develop mobile payment guidelines for various participants in the Canadian mobile commerce ecosystem.

In response to this request, the Canadian Bankers Association coordinated the development by Canadian banks and credit unions of a Canadian Near-Field Communications ("NFC") Mobile Payments Reference Model (the "Reference Model"). The first version was published on May 14, 2012.

This Reference Model provides a detailed blueprint for how NFC mobile payments can be offered in Canada, how open mobile wallets should be and how consumer privacy will be

assured, including guidelines on how information is exchanged amongst various parties to a transaction including financial institutions, payment card companies, telecommunications companies and merchants.

The Reference Model will enable the development of software applications that allow consumers to enter into the same transactions using their mobile phones that they currently engage in using their payment cards. It will also allow merchants to accept such payments using their current hardware at the point of sale. Other participants, not just banks and credit unions, will be able to participate in the mobile payments market by building mobile wallet applications for consumers such as government issued identification, library cards, transit passes, and merchant loyalty cards.

The fundamental principle underlying the Reference Model is that each participant must protect adequately end user and merchant data. Access to and usage of the data must be disclosed to the end user and the end user's permission must be expressly granted.

The Reference Model focuses on payments executed through NFC technology using a handheld mobile device. Since NFC-based mobile payments or contactless payments require the mobile device to be in close proximity to the reader, such payments require the integration of hardware and software on the mobile device. Accordingly, the Reference Model provides a framework for the interaction between the different ecosystem participants.

The Reference Model focuses on the following software (wallet application, payment application and payment credentials) issues:

- Wallet and payment application features, functionality and security.
- Enablement and lifecycle management including the setup steps needed to install a mobile wallet and payment application on a mobile device, securely bind the applications and manage these applications over customer lifecycle events (e.g. lost or stolen phones).
- Transaction processing.
- Loyalty and reward program integration with NFC mobile payments.
- Data & Security.

Following the release by the Canadian banking and credit union industry of this landmark Reference Model, CIBC and Rogers Communications Inc. announced plans to launch a joint NFC mobile payments service in Canada. The service, due to launch "later this year", will enable consumers to store multiple Visa and MasterCard CIBC credit cards on a SIM-based secure element in a Rogers NFC phone and use them to make payments at any merchant equipped with a contactless POS terminal.

Litigation Update

Begum v. MBNA Canada Bank

A recent decision of the Court of Quebec (Civil Division), *Begum vs. MBNA Canada Bank*, rendered by Mr. Justice Christian M. Tremblay, sheds light on the legal rules in Quebec with respect to a consumer's liability for use of his credit card where the consumer has alleged loss or theft of the card. The Court considered the application of sections 123 and 124 of the Quebec *Consumer Protection Act*, which, like similar provisions in other Provinces' consumer protection laws, provides that a consumer's liability for debts arising from use of a credit card is limited to $50.00 where the card has been lost or stolen.

In the Begum case, persons claiming to be the plaintiff and her husband telephoned MBNA Bank to advise that she would be travelling to Bangladesh. She indicated the number of the

card and certain personal information requested by the Bank to permit use of the card in that country. The card was used there to buy jewelry and other consumer items.

The plaintiff claimed that she was not in Bangladesh when the purchases were made and stated that the recorded voices requesting unblocking of the cards (for use in Bangladesh) were not hers.

She further argued that the only time she used the card before the alleged unauthorized use, apart from paying the minimum balance to maintain a demand loan of $6,500.00, was at a restaurant in Montreal. The card in question had not been stolen physically and indeed had been deposited as an exhibit in the hearing. However, the bank demonstrated that the card had been swiped in Bangladesh. Plaintiff argued that the card must have been "cloned", i.e., a counterfeit card was made up using personal information stolen from her. The implication was the card may have been cloned from swiped information obtained at the restaurant in Montreal.

The Bank led evidence that there had been no cases of cloning or alleged cloning involving this restaurant before, and the alternate explanation, that the card was stolen from plaintiff, copied and then returned to her without her knowledge, was not plausible. Other evidence, including similar alleged unauthorized use of credit cards belonging to family members of the plaintiff in the same country in the same period, as well as the relative scarcity of the equipment necessary to clone cards, convinced the Court that unauthorized cloning had not occurred.

The Court noted that earlier case law in Quebec had established that a cardholder seeking to show that his card was lost or stolen has the legal burden of proof. This means he must show on a balance of probabilities that it is more likely the card was stolen or lost, than if the contrary was the case. The Court decided that plaintiff had not satisfied this burden after a careful assessment of the evidence submitted. The Court noted that it was not sufficient for the plaintiff to affirm that that the card was lost or stolen without giving any plausible explanation of how the fraud took place and how so much personal information about her had been obtained by the fraudsters. The bank, on the other hand, had set out precise and concordant elements to show that the card had not been cloned and that the fraudsters knew all the personal information about the plaintiff which would allow the unblocking of the card. What is more, the plaintiff's conduct after the fraud was not consistent with that of individuals who have been defrauded.

While a consumer whose card is lost or stolen cannot be required to pay the charges beyond $50.00, (a policy decision of the legislators long in place and not in question), this decision shows that our courts are robust to require persons alleging loss or theft of their credit card to show how it could have occurred. There must be some reasonable evidence that the card was stolen or cloned. In the Begum case, plaintiff was held not to have proved any such circumstances and other facts before the court convinced it that the card had not been cloned and that the activity on the card had not been unauthorized.

Marcotte v. Bank of Montreal et al

On June 11, 2009, in a decision by the Superior Court of Quebec, the court ordered nine Canadian banks and Desjardins to pay over $200 million to the members of the classes named in those class actions. The court found that:

- Provincial consumer protection legislation applies to federally regulated banks in matters of credit and credit cards notwithstanding exclusive federal jurisdiction over banking under Section 91(15) of the *Constitution Act, 1867* and the doctrine of paramountcy. The court held that neither foreign currency exchange nor the extension of credit through credit cards are part of core banking activities and were thus not included in the activities over which the (federal) Parliament is given

exclusive jurisdiction. The Court therefore concluded that banks are obligated to comply with applicable provincial legislation in providing such services.

- The Court further held that there was no operational conflict between the CPA and the federal Bank Act or other applicable federal legislation, and the doctrine of "paramountcy" did not apply such that Parliament's efforts to regulate these areas were not frustrated by the application of the CPA.

- Foreign currency conversion fees are "credit charges" within the meaning of the Québec *Consumer Protection Act* (CPA). The banks and Desjardins failed to disclose such fees and were found to have contravened certain provisions of the CPA.

- Consequently, members of the class are entitled to the reimbursement of foreign currency conversion fees that were charged illegally and punitive damages totalling approximately $200 million.

This decision is currently under appeal. If the decision is not reversed, banks may find that a wide swath of provincial legislation which they had previously regarded as inapplicable to them under will now apply to federally regulated banks.

Bill C-38- Jobs, Growth and Long-term Prosperity Act

An Act to implement certain provisions of the budget tabled in Parliament on March 29, 2012 and other measures, also known as the *Growth and Long-term Prosperity Act*, received Royal Assent on June 29, 2012. One interesting section (section 525 of Division 36, Part 4), amends the *Bank Act* to add a preamble to that Act, perhaps in an effort to strengthen the Canadian banks' view that the federal Parliament has exclusive jurisdiction over banking under Section 91(15) of the Constitution Act, 1867 and accordingly, provincial legislation which purports to legislate relative to banks and banking is not applicable to banks. The section, as enacted, reads as follows:

"Preamble

Whereas a strong and efficient banking sector is essential to economic growth and prosperity;

Whereas a legislative framework that enables banks to compete effectively and be resilient in a rapidly evolving marketplace, taking into account the rights and interests of depositors and other consumers of banking services, contributes to stability and public confidence in the financial system and is important to the strength and security of the national economy;

And whereas it is desirable and is in the national interest to provide for clear, comprehensive, exclusive, national standards applicable to banking products and banking services offered by banks;".

Jones v. Tsige

In a decision of the Ontario Court of Appeal rendered on January 12, 2012, the Court recognized a common law cause of action for invasion of privacy. Before this decision, there had been doubt whether such protection existed in Canadian common law.

In that case, a Bank of Montreal employee, Ms. Tsige, surreptitiously and contrary to bank policy, accessed the banking records of Ms. Jones, approximately 174 times over a span of four years. Ms. Tsige indicated that she was involved in a financial dispute with the Ms. Jones' former husband and had accessed the accounts to confirm whether he was paying child support to Ms. Jones.

The appeal was taken from a decision of the Ontario Superior Court of Justice which concluded that there was no free-standing right to privacy under the Charter or at common law, and further, that given the existence of specific privacy laws (statutes) protecting certain elements of one's privacy, any expansion of those rights should similarly be dealt with by statute rather than through the courts via the common law.

The Court of Appeal reversed that decision and held that it was appropriate "to confirm the existence of a right of action for intrusion upon seclusion" or in other words recognized a common law action for breach of privacy.

In defining the new tort, the court cited the following as its rationale:

1. The case law was generally in support of the existence of such a cause of action.
2. "The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic data bases render our most personal financial information vulnerable."
3. It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form.
4. The Court was presented "with facts that cry out for a remedy."

The key features of the new cause of action are:

1. The defendant's conduct must be intentional or reckless.
2. The defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns.
3. A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.
4. Proof of harm to a recognized economic interest can be but is not a necessary element of the cause of action.

The Court noted some important limitations on this cause of action, as follows:

- A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy.
- Claims from individuals who are overly sensitive or unusually concerned about their privacy are excluded.
- Only intrusions into "financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.", will be protected.
- Privacy claims may give rise to competing claims such as freedom of expression and freedom of the press. In such cases the protection of privacy "will have to be reconciled with, and even yield to, such competing claims."

The Court held that "proof of actual loss is not an element of the cause of action for intrusion upon seclusion" and that in a case such as the one before the Court where there was no actual loss, the damages must be assessed on the basis of "symbolic" or "moral" damages. Furthermore, aggravated or punitive damages may be appropriate in exceptional cases.

The Court adopted the following guiding factors when assessing damages:

- The nature, incidence and occasion of the defendant's wrongful act.
- The effect of the wrong on the plaintiff's health, welfare, social, business or financial position.
- Any relationship, whether domestic or otherwise, between the parties.
- Any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong.

- The conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.

The Court considered that an appropriate cap on damages in such cases was $20,000 and that the case before it fell in the middle of the range, and assessed damages at $10,000.

Implications of the Decision

This decision may have implications for organizations currently subject to the *Personal Information Protection and Electronic Documents Act* or substantially similar privacy legislation. Organizations may be subject not only to the statutory duty to protect personal information that they collect, use or disclose in the course of commercial activities, but to a common law duty as well. It may also increase the risk of class actions based on invasion of privacy.

Competition Bureau Alleges Anti-Competitive Conduct by Visa and MasterCard

On May 8, 2012, the Commissioner of Competition's case against Visa and MasterCard rules began before the Competition Tribunal.

The Competition Bureau announced in December 2010 that it had filed an application with the Competition Tribunal to strike down what it considered to be restrictive and anti-competitive rules that Visa and MasterCard impose on merchants who accept their credit cards. The Commissioner alleged that these rules have effectively eliminated competition between Visa and MasterCard for merchants' acceptance of their credit cards, resulting in increased costs to businesses and, ultimately, consumers.

The Bureau is challenging Visa and MasterCard's rules under the price maintenance provisions of the *Competition Act*. The Bureau launched its investigation in response to complaints by merchants and initiated formal inquiry in April 2009.

The following is a synopsis of the Competition Bureau's opening statement taken from the Competition Bureau's website (see http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03466.html):

"Although credit cards are part of our everyday lives as consumers, Canadians are largely unaware of the significant costs merchants incur by accepting Visa and MasterCard credit cards. Each year, Canadian merchants pay more than $5 billion in hidden credit card fees on Visa and MasterCard transactions. Those significant fees are reflected in higher prices paid by all Canadian consumers, including customers who do not even use credit cards, and pay with less expensive methods of payment such as an Interac debit card or cash.

Credit card fees in Canada are among the highest in the world. Canadian merchants who accept Visa and MasterCard credit cards must pay a fee from 1.5 to more than 3 percent of each purchase, nearly twice as much as their counterparts pay in Europe, New Zealand and Australia, but slightly less than in the United States.

By contrast, the card acceptance and processing fee paid by merchants in the case of an Interac debit transaction is a flat fee of approximately 12 cents, regardless of the value of the purchase. To provide a practical example, a 2.5 percent hidden fee on a $200 barbecue is $5, but if a debit card is used for the same purchase, the fee is 12 cents. The credit card cost is more than forty times higher than the debit card cost.

To protect the more than $5 billion in hidden credit card fees paid by Canadian merchants each year, Visa and MasterCard have imposed on merchants a number of rules that harm competition. The rules challenged by the Bureau prohibit merchants from encouraging

consumers to consider lower-cost payment options such as cash or debit, and prohibit merchants from applying a surcharge to a purchase on a high-cost card. Further, once a merchant agrees to accept one of Visa or MasterCard's credit cards, that merchant must accept all credit cards offered by that company, including cards that impose significant costs on merchants, such as premium cards. Because retailers cannot charge a higher price for higher-cost premium credit cards, even though they are substantially more expensive than other methods of payment, merchants are forced to increase prices for all customers in order to reflect the more than $5 billion in hidden credit card fees paid by merchants each year.

Because Visa and MasterCard's anti-competitive rules prevent merchants from encouraging customers to use lower-cost payment methods, Visa and MasterCard are able to maintain high prices for their services, prices that are passed on to all consumers. Removing the anti-competitive rules will introduce some competition between Visa and MasterCard to secure merchants, which will in turn lead to lower credit card costs for merchants and lower prices for consumers."

New Consumer Complaints Requirements for Banks

On July 6, 2012 the Minister of Finance announced new proposed regulations for banks and authorized foreign banks regarding consumer complaints. The regulations, entitled *Approved External Complaints Bodies (Banks and Authorized Foreign Banks) Regulations* (the "Regulations"), set out standards that external complaints bodies must meet in order to maintain approval to settle consumer complaints. The Regulations also set out new obligations for banks and authorized foreign banks. For more information, see the Department of Finance's publication entitled *Backgrounder*: *Approved External Complaints Bodies (Banks and Authorized Foreign Banks) Regulations* at: http://www.fin.gc.ca/n12/data/12-079_1-eng.asp.

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.