GILLMAN & GILLMAN
Barristers & Solicitors

Volume 1, No. 3

Spring/Summer 2005

The Financial Services Regulatory Report

Recent Privacy Developments: a Wake-up Call to Businesses!

In the wake of a much publicized privacy breach by a major financial institution, the Office of the Privacy Commissioner (OPC) is urging all Canadian businesses to assess their privacy management policies and practices, and meaningfully address any shortcomings.

Lessons Learned

The potential for adverse negative publicity, civil damages and regulatory penalties suggest that companies that collect, use or disclose personal information must exercise a high degree of caution and compliance.

Adopting a privacy policy does not, in and of itself, make a business privacy-compliant. Policies must be implemented in meaningful and practical ways. Organizations must ensure, for example, that, on an ongoing basis all employees are aware of and adhere to their privacy policies. This means that where privacy breaches have occurred employees must bring them to the immediate attention of the organization's designated privacy officials.

Secondly, organizations should implement a procedure to notify customers when their personal information is inadvertently disclosed. This is not currently a requirement of the federal *Personal Information Protection and Electronic Documents Act*.

However, such measures are now part of the exacting data privacy legislation enacted in at least six US states in response to high profile privacy breaches by major corporations in that country. In addition, under the US Gramm-Leach–Bliley Act of 1999, banks and thrifts must inform regulators of any compromise of sensitive customer information. Moreover, in the event of such compromise or its likelihood, customers themselves must be notified in a "clear and conspicuous manner".

American legislative developments may suggest that ultimately similar requirements will be adopted here. Canadian privacy officers should consider implementing a mechanism *now* to notify affected customers that the disclosure or misuse of customer information has occurred or is reasonably possible.

Finally, organizations must exercise sufficient due diligence in attempting to retrieve misdirected personal information. Privacy officers should, therefore, implement a practice to require such retrieval and consider obtaining a written acknowledgment that the recipient will not use, disclose or copy the information that they have inadvertently received.

By adopting proactive steps such as are mentioned above (which are not exhaustive, and would need assessment and tailoring to the organisation concerned), organizations can foster more effective corporate privacy risk management practices and procedures.

New Secure Electronic Signature Regulations under *the Personal Information Protection and Electronic Documents Act*

Part II of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provides a framework to permit federal statutes and regulations to accommodate electronic alternatives to paper-based means of communication. For some types of documents that need to be generated electronically (such as sworn statements, statements declaring truth, witnessed documents, original documents and sealed documents), Part II requires a *secure electronic signature*.

A *secure electronic signature* is defined as an electronic signature that results from the application of a technology or process prescribed by regulations (subordinate legislation) made under subsection 48(1) of the PIPEDA. Section 48(1) describes the characteristics of a secure electronic signature and grants authority to the Governor-in-Council (the Cabinet) to set out the specific technologies or processes for the purpose of the definition.

On the fifth anniversary of PIPEDA becoming law, these regulations were finally enacted. However, the only technology that the Regulations currently prescribe to meet the criteria set out in the definition of *secure electronic signature* is "public key based technology".

Financial institutions should consider the impact of this development in light of their own businesses. What are the opportunities created thereby? What will their impact, if any, be on the forthcoming scheduled major revision of federal financial institutions legislation?

2006 Financial Institution Legislative Review

A consultation paper, entitled "*An Effective and Efficient Legislative Framework for the Canadian Financial Services Sector",* was released as part of the federal government's Budget 2005. This has launched the process leading to the anticipated 2006 financial institution legislative review. The consultation period runs until June 1, 2005.

This summer, Ottawa will pursue and complete the policy review. Proposals and a White Paper will be released in the fall. Following a process of committee hearings, it is anticipated that reforming legislation will be introduced in the House of Commons in early 2006 with a view to having it become law by the deadline of October, 2006.

In its review, the Government is considering making selective changes to financial institutions' governing laws, aiming to achieve three principal goals:

- Enhancing the interests of consumers
- Increasing legislative and regulatory efficiency
- Adapting the framework to new commercial and business developments

The following are examples of areas under review and where the Government is seeking specific industry input:

- The disclosure regime for customers, particularly in the areas of investment-focused products, registered plans, deposit accounts and complaints-handling procedures.
- How to best address disclosure and assignment of liability for all forms of electronic payments transactions.
- Establishing maximum hold periods for cheques.

- The scope of the foreign bank entry framework, its core principles and how to simplify the mechanics of foreign bank entry.

- Streamlining current regulatory requirements for more routine transactions.

Canadian Payments Association (CPA) Developments

CPA Approves New Rule to Facilitate On-Line Payment Services

A new CPA Rule, Rule E2, *Exchange for the Purpose of Clearing and Settlement of Electronic On-Line Payment Items* came into effect on February 3, 2005. It will facilitate new on-line payments services that will allow consumers to pay for purchases directly from their bank account via the Internet.

Under the Rule, the customer's financial institution is responsible for directly authenticating the consumer (through his/her on-line banking user ID and password) and obtaining the consumer's authorization for each on-line payment transaction.

Consumers and merchants will benefit in many ways:

- Consumers will not provide their user ID or password to a merchant or other on-line party, thereby better protecting a consumer's privacy.
- Using a credit card for on-line transactions will no longer be the only method of conducting on-line transactions.
- Merchants can offer a new payments option to on-line customers.
- Merchants that offer this method of payment will have greater finality of payment. Once the transaction is approved, the financial institution will debit the buyer's account for the value of the transaction and provide settlement. As a result, the merchant will be assured that the funds cannot be subsequently recalled by the customer.

In conjunction with the passage of this Rule, the CPA Board issued a Statement of Policy encouraging members to apply the relevant principles of the *Canadian Code of Practice for Debit Card Services* and to subscribe to a fair and transparent framework of consumer protection.

CPA Published a New Cheque Specification as Part of the Transition to Image-Based Clearing

As part of an industry-wide initiative to capture images of cheques in order for them to be cleared electronically, the CPA has announced a new cheque specification (Standard 006).

Under the CPA's *Truncation and Electronic Cheque Presentment (TECP) Project*, an image of each cheque will be captured electronically by the financial institution that accepts the cheque and then sent electronically to the drawer's bank. At the heart of this project is the need to make the imaged cheque more "photogenic" and to ensure key elements are placed in standardized locations.

The new cheque specification requirements will come into effect on December 31, 2006.

Changes to the cheque design include:

- Adoption of a numeric date field.
- Technical specifications to ensure good document design and to facilitate taking good "pictures" of the front and reverse sides of each cheque. These specifications include requirements to address such matters as background colours and design and choice of ink colours.
- Defining consistent positions for key fields.

As a result, businesses are encouraged to look at how they currently design and source their cheques and adopt processes to make them conform to the new requirements. Those businesses which print their own cheques should provide pre-production samples to their financial institution to ensure they meet the new specifications.

Although the benefits of image-based cheque clearing will vary for financial institutions and businesses alike, the range of potential benefits includes:

- Easier spotting of post- or stale-dated cheques.
- Better combating fraud through automated signature verification and encrypted bar codes.
- Reduced costs of transportation and storage of physical cheques.
- More timely account reconciliation.
- Faster tracing of cheques.
- Better customer service in responding to customer inquiries concerning cheques.

If you require assistance on how any of these regulatory or legislative developments affect your organization, please call financial institutions legal specialist, Libby Gillman at 416.418.7204 or contact her at libbyg@lawgill.com

The Financial Services Regulatory Report is published periodically to keep interested parties 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.

A Corporate Guide to Privacy – Checklist to See How You Measure Up

Organizations doing business in Canada must ensure that they have the technical infrastructure, legal and business policies, procedures and ongoing monitoring to protect the personal information of their customers and employees. Companies must work hard to earn and maintain the trust their customers place in them. Companies that adopt comprehensive privacy and security policies and procedures reassure their customers that their personal information is valued and protected. This commitment reinforces valued customer relationships and creates a tremendous opportunity for businesses to gain competitive advantage, strengthen their brands and capitalize on the e-business explosion. Also, doing "due diligence" in this area will likely minimize the legal fallout should a privacy problem occur.

Organizations Should Take Immediate Steps To:

- √ **Use qualified professional advisers with proper credentials in privacy and information security.**
- √ **Conduct or update a comprehensive privacy and security risk assessment (audit) to identify risks and vulnerabilities with specific recommendations to mitigate risk, close gaps and advise on best practices. Assess the likelihood and potential damage of these risks, considering the sensitivity of the information and other factors.**
- √ **Review and evaluate the sufficiency of policies, procedures, customer information systems and other arrangements to control the risks, including any current privacy/security policies and procedures.**
- √ **Develop a plan to bring these up to the standards of privacy and security "best practices", as well as existing and emerging privacy legislation, including the federal *Personal Information Protection and Electronic Documents Act* and the numerous, applicable provincial privacy laws.**
- √ **Consider the technical, legal and operational implications of these privacy and security requirements and integrate the privacy initiative into the organization's marketing plan and value points.**
- √ **Develop a consensus-based action plan with solutions and remedies to protect information, information disclosure and retention systems.**
- √ **Establish a measurement and reporting regime to identify, measure, manage and report on privacy and security risks on an ongoing basis. Regularly review the organization's privacy and security policies and procedures to make improvements as needed to retain and increase their competitive edge.**
- √ **Consider the privacy and security aspects of each new business initiative and relate/integrate them into the existing privacy policies. For example, consider the privacy and security requirements of data warehousing (including cross-border), data mining and customer relationship management projects.**
- √ **Assure customers and the marketplace that the organization has complied with applicable legislation, developed *and implemented* comprehensive privacy/security policies and procedures.**