GILLMAN & GILLMAN
Barristers & Solicitors

Volume 2
No. 1
Spring, 2006

The Financial Services Regulatory Report

U.S. Regulators Focus on Authentication in an Electronic Banking Environment – Are Canadian Regulators Far Behind?

In October, 2005, the Federal Financial Institutions Examination Council ("FFIEC"), a group of U.S. financial institutions regulators,* released an updated "guidance" on authenticating the identity of customers using Internet-based financial services. Although the guidance is focused on the risks and risk management techniques associated with the Internet channel, the principles are applicable to all forms of electronic banking activities.

The guidance, *Authentication in an Internet Banking Environment*, was issued to reflect recent significant legal and technological developments in protecting customer information, preventing or reducing identity theft and fraud, and improved authentication technologies and other risk mitigation strategies. When releasing this guidance, the FFIEC stated:

> "The continued growth of Internet banking and other forms of electronic banking activities and the increased sophistication of threats to those environments have resulted in higher risks for financial institutions and their customers. An effective authentication system is necessary for financial institutions' compliance with requirements to safeguard customer information; to prevent money laundering and terrorist financing; to reduce fraud and the theft of sensitive customer information, often the precursor to identity theft; and to promote legal enforceability of financial institutions' electronic agreements and transactions."

The guidance, which replaces the FFIEC's *Authentication in an Electronic Banking Environment* issued in 2001, highlights the need for risk-based assessments to identify the types and levels of risk associated with Internet banking applications. Where risk assessments indicate that single-factor authentication (PIN/password only) is inadequate, financial institutions are advised to implement multi-factor authentication, layered security or other controls to mitigate these risks.

The guidance also addresses the need for:

- ✓ regular monitoring of unauthorized access to computer systems and customer accounts,
- ✓ reporting unauthorized access to senior management and appropriate regulatory and law enforcement agencies,
- ✓ effective customer awareness programs.

The guidance does not endorse any particular technologies, but rather sets a framework for authentication best practices. This framework must be considered in light of the applicable

---

* FFIEC is comprised of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision.

legal framework. In Canada, this is the ensemble of federal and provincial financial institution laws and the supervisory system of OSFI and other regulatory bodies.

In the absence of similarly focused Canadian regulatory guidelines, Canadian financial institutions are well advised to regard the guidance as a statement of current authentication best practices. Accordingly, they should consider implementing the risk identification and risk mitigation techniques recommended therein.

Privacy Compliance: Risks and Rewards

Last year, at least 118 privacy and data breaches compromised the personal information of more than 57 million people in the U.S. and Canada. To date in 2006, there have been at least 50 such incidents, potentially affecting more than 21.3 million individuals.*

In one case last year, the Canadian Privacy Commissioner called a bank's privacy practices a "failure at the *most basic organizational level*" and a "wake-up call to business".

In another instance, a major U.S. commercial data service provider was duped into releasing sensitive information on over 160,000 customers *including Canadians*. In that case, the U.S. Federal Trade Commission announced that the offending company agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and record handling procedures violated consumers' privacy rights and federal laws. The settlement requires the company to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes. It must also undergo an audit every two years by an independent security professional.

In another case, a bank lost computer data tapes containing the personal information of 1.2 million federal employees including some members of the U.S. Senate. In yet a further instance, the Wall Street Journal revealed numerous mutual funds reported data security breaches. And the list goes on….

Examples of Canadian and American Privacy Breaches and Their Impact*

Date Made Public	Type of Company	Breach	Number of Individuals Potentially Impacted
2004-2205	Canadian bank	Misdirected faxes	Unknown
2002-2004	Canadian bank	Misdirected faxes	Unknown
September 12, 2003	Canadian bank	Obsolete computer servers containing customer data sold to third party	350
April 28, 2005	U.S. Bank	Dishonest insiders	676,000
Feb. 25 , 2005	U.S. Bank	Lost backup tape	1,200,000
June 16, 2005	Card system service provider	Hacking	40,000,000
Feb. 15, 2005	Card system service provider	Bogus accounts established by ID thieves	160,000 (including many Canadians)
April 14, 2005	Retailer/Bank	Hacking	180,000
April 20, 2005	On-line discount broker	Lost backup tape	200,000
June 6, 2005	U.S. bank	Lost backup tapes	3,900,000

*Source: Privacy Rights Clearinghouse website at: http://www.privacyrights.org/ar/ChronDataBreaches.htm

These privacy incidents have coloured the expectations and perceptions of consumers, businesses, and regulators across the globe and form key features of the privacy landscape. They cause some businesses to be reactive while others are proactive.

A survey conducted by the Ipsos Group in the U.S. reported that the percentage of Americans using online banking services has stalled at 39% after a period of impressive growth. The primary reason: 73% of consumers said they were avoiding online banking because of concerns about the poor job banks were doing to protect their privacy. (Source: *The Profits in Privacy*, CIO Magazine, March 15, 2006, http://www.cio.com/archive/031506/privacy.html.

In another survey conducted by EDS Canada last year, consumers were asked how they would respond if "there was a security breach at your bank or financial institution and your personal information was compromised." Calling this "the most significant finding of the study", EDS reported that 54% of customers would discontinue *all* banking activity until the crisis was resolved and 38% would discontinue *online* banking activity until the crisis was resolved. (Source: EDS White Paper: *EDS Canada Financial Services Privacy and Customer Relationship Management Survey* May 2005)

Regulators increasingly see the number of incidents as evidence that privacy and security issues are not being taken seriously by some companies. As a result, regulators are responding.

In Canada, the federal Privacy Commissioner has suggested that she will make more and better use of the existing audit powers in section 18 of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Armed with increased resources, the Privacy Commissioner has stated her office "reasonable grounds" for an audit in several organizations.

She is also considering whether additional powers of enforcement should be made available to the federal Privacy Commissioner.

In her speech to the 7th Annual Privacy and Security Conference (Victoria, B.C. February 9, 2006), the Privacy Commissioner stated that:

> "We need to strengthen our ability to influence changes in attitudes and behaviours within the Canadian commercial sector so that commercial organizations not only comply, but even exceed, the principles enshrined in *PIPEDA*. We intend to do this by several means, including working with business, industry and professional associations on privacy guidelines, standards and self-assessment tools, and by promoting exemplary practices in privacy protection and personal data management practices. *This also means getting the laggards in the commercial sector – some banks spring readily to mind – to educate their employees about the importance of privacy and how to protect it.*
>
> *They have not done so enough, in my view, and there have been too many lapses of security of personal information as a result. Organizations that have been covered by PIPEDA since its first phase came into force in 2001 no longer have any excuse for failing to bring their privacy practices up to snuff. I am particularly concerned that organizations covered by PIPEDA since 2001, and the banking sector is not alone, seem to be so vulnerable to employee misuse of customer personal information. Has training been neglected? Are supervisory procedures deficient? Does no one check the data trail periodically?"*

In the U.S., t*wenty-two* States have passed laws requiring that individuals be notified of security breaches. Congress is considering several bills this year in which security breach notices would be mandated nationwide. Experts say that some kind of legislation on data security and privacy will almost certainly be passed in the U.S. this year.

Privacy Risks

Not only do financial services providers risk incurring large monetary penalties and civil damages, a failure to address privacy adequately negatively affects customer and employee relationships, brand and reputation and therefore, shareholder value can be compromised.

The Rewards

While the risks of ignoring or minimizing privacy requirements are now evident, proper attention to privacy compliance and risk management can glean many rewards. Companies that adopt comprehensive privacy and information security policies and implement them in meaningful ways reassure their customers that their personal information is valued and protected. This maintains and reinforces valued customer relationships and loyalty. It creates a tremendous opportunity for businesses to gain competitive advantage and to strengthen their brands and reputation.

An Action Plan

Financial institutions should *act now* to ensure that they have effective and efficient privacy compliance programs. They should:

- ✓ Conduct a comprehensive, enterprise-wide privacy and security risk assessment to identify material risks and vulnerabilities.
- ✓ Assess the likelihood and potential damage of these risks, considering the sensitivity of the information.
- ✓ Review and evaluate the sufficiency of current and proposed policies, procedures, customer information systems and other arrangements to preclude and control risks.
- ✓ Develop a consensus-based action plan providing solutions and remedies to close gaps and mitigate risks.
- ✓ Consider the technical, legal and operational implications of these privacy and security requirements.
- ✓ Implement appropriate risk mitigation strategies.
- ✓ Establish a benchmarking system to identify, measure, manage and report on privacy and security risks.
- ✓ Regularly review their privacy and security policies and procedures to make improvements as needed.
- ✓ Track and assess relevant changes in technology, the sensitivity of its customer information, internal or external threats and applicable laws and regulations.
- ✓ Consider the privacy and security aspects of each new business initiative.
- ✓ Educate their employees about the importance of privacy and how to protect it.

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.