

PRIVACY LIABILITY AND INSURANCE

*Prepared by Murn Meyrick, Senior Vice President, Corporate Counsel
Executive Risk Insurance Services*

OVERVIEW

The growth and importance of information systems and technology in our every day lives is incontrovertible. Governments and businesses now collect and store sensitive private information relating to their customers and employees on a scale previously unimaginable. Technological advances allow quick and easy access to this personal information from around the world. Although the benefits in terms of convenience and efficiency are obvious, the associated privacy risks are substantial.

News headlines around the globe highlight the increasing frequency and severity of privacy breaches. The most egregious example to date is the incident at Winners/HomeSense where at least 45.7 million customers' credit and debit card accounts were compromised in the United States and Canada when hackers stole customer information of the U.S. parent company TJX Cos. Ltd. (TJX). The breach was disclosed in January 2007 although it is believed the hacking activity began in July 2005. The resulting loss to TJX was staggering, including settlements with credit card companies for \$65 million, settlements with U.S. and Canadian regulators in respect of cash benefits, ID theft insurance, reimbursements for out-of-pocket costs, implementation of safeguards and retention of a third-party auditor to undertake vulnerability testing of their system for the next 20 years. In the aftermath of the breach, TJX and its board of directors is facing litigation from stakeholders including consumers, with whom a tentative settlement was reached in July 2008; banking associations; and shareholders. Total costs of the breach are estimated by technology analysts to exceed \$1 billion.

In March 2008, in another high-profile data breach in the United States, up to 4.2 million credit and debit cards used at Hannaford Bros. Co. grocery stores in the northeast United States and Florida were accessed, resulting in a multi-million dollar tab for the replacement of the compromised cards and at least 1,800 cases of fraud. Consumer class action lawsuits followed shortly after the breach was revealed.

There is no shortage of high-profile privacy breach incidents in the United Kingdom. In late 2007 the Inland Revenue lost unencrypted discs containing sensitive information of 25 million British citizens. In another incident, Nationwide Building Society sustained the loss of a laptop computer containing unencrypted sensitive customer data. This led to notification letters being sent to all 11 million individuals potentially affected and a £980,000 fine being levied by the U.K. Financial Services Authority for inadequate systems and controls to address information security risk.

Canada has similarly seen an explosion in breach incidents which have more than doubled since 2006, according to a 2008 national survey of Canadian IT security executives by CA Canada.¹ In her annual report released in June 2008, the federal Privacy Commissioner noted that "The year 2007 will no doubt be remembered in the privacy world as the year of the data breach . . . with the size of some of the data spills reported around the globe staggering".²

In the past two years alone, Canadian breach incidents have included the loss of a computer hard drive loaded with the private information of thousands of clients of a subsidiary company of the Canadian Imperial Bank of Commerce, a web server "glitch" at Canada Post that allowed unauthorized access to the login records of scores

¹ CA Canada 2008 Security and Privacy Survey, June 2008.

² Office of the Privacy Commissioner of Canada, Annual Report to Parliament 2007 (Ottawa: Minister of Public Works and Government Services Canada, 2008).

of small businesses, a security flaw in Passport Canada's Web site that allowed easy access to the personal information—including social insurance numbers—of new passport applicants, and the theft of personal information of 3.3 million Bell Canada customers that led to the arrest of a suspect in Montreal. Most recently, DaimlerChrysler Financial Services Canada Inc. admitted that a courier service it used had lost a data tape containing the sensitive personal information of thousands of Canadian auto customers, which has led to the commencement of a class action. Furthermore, in July 2008, an investigation by Visa Canada was launched of suspected credit card fraud at Toronto Pearson International Airport's self-service check-in kiosks. This news prompted WestJet to disable the credit card readers at its kiosks as a precautionary matter.

With the growing incidence of privacy breaches around the globe the potential losses are enormous. As a result, companies and their in-house counsel are recognizing identity and security breaches as a key business threat and are closely examining risk management solutions to reduce their exposure, including identifying new insurance solutions.

Legislative Background

The Advent of Privacy Legislation

The growth and importance of IT systems and technology throughout the 1980s and 1990s resulting in the collection, storage, and transmission of data in ways that had not been historically contemplated meant that existing legislation became largely outdated and unresponsive to ever-expanding e-commerce risks. A growing realization around the globe of the need for modern privacy legislation has led to the extensive development of privacy-specific laws that continue to be under debate and continue to evolve. Such privacy legislation worldwide contains many common themes: in particular, all such laws seek to address the collection, storage, and use of "personal information" by both government agencies and the private sector. All seek to outline appropriate technical and organizational measures to protect such data. "Personal information" is typically described as data that can be used to identify a living individual, with a focus upon financial and health care related data. Most laws seek to outline the rights of individuals and potential sanctions for breach.

PIPEDA and Its Effects

Initial legislative efforts focused on the rights of individuals to know what personal information was being stored by an organization and to gain access to it, but little or no rights were established for individuals to know when such information was tampered with or inappropriately leaked to a third party as a result of a security or administrative breach. This is changing. The United States has led the way in implementing breach notification laws, mandating that organizations inform individuals potentially affected by a breach. At present, approximately 42 states mandate breach notification, with each of those states having their own laws. As a general rule, the law of the state where a harmed citizen resides will apply to a breach. Although many of the states follow the California model,³ which pioneered the idea of breach notification in the United States, many of the state laws contain significant differences. Headline grabbing security breaches around the globe have put pressure on legislators in other jurisdictions to follow suit.

In Canada, the privacy of personal information is protected, inter alia, in federally regulated workplaces under the Personal Information Protection and Electronic Documents Act⁴ (PIPEDA) and, in the provinces of Alberta, British Columbia, and Quebec, under "substantially similar" privacy Acts (see, Map of Canadian Privacy Laws, in Schedule A – attached). A review of PIPEDA by Industry Canada that commenced in late 2007⁵ has resulted in a strongly

³ Cal. Civ. Code SB 1386.

⁴ S.C. 2000, c. 5.

⁵ Industry Canada, Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics — Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA) (Ottawa: Publishing and Depository Services, Public Works and Government Services Canada, 2007).

supported recommendation for mandatory data breach notification. The proposal prescribes that in the event of a data breach where an organization determines there is a high risk of significant harm to individuals resulting from the breach, the organization is required to notify affected individuals as soon as is reasonably possible after detection of a breach. Although debate continues over the threshold trigger for the notification, it appears likely that some form of notification requirement will be implemented before the end of 2008. It is anticipated that provincial and public privacy laws will follow suit. The effect of a mandatory breach notification would be increased public awareness for both affected individuals and regulators, with the likelihood of increased regulatory intervention and consumer litigation.

Identity Theft

Other legislative efforts in Canada have focused on addressing one of the fastest-growing crimes in North America—identity theft—which has become both rampant and lucrative.⁶ Bill C-27,⁷ which was introduced in the fall of 2007, received second reading on January 30, 2008, and is currently before Committee, would, if passed, make it illegal to obtain, possess, or sell other people’s identity information in order to commit a crime. The goal of the legislation is to act as a tool to prevent fraud before it happens. In addition to provincial and federal privacy legislation there exists a framework of additional statutory and common laws, as well as industry-specific standards and contractual obligations, that work together to form the rules safeguarding personal information in Canada.

PRACTICAL APPLICATION

Which Companies are at Risk?

Sectors

Identifying a business’s risk profile for loss arising from a privacy breach requires an analysis of a number of factors. Although any company that collects and stores its employees’ or customers’ personal information is exposed, recent Canadian statistics⁸ reveal that the following industries are particularly at risk:

- financial institutions;
- telecommunications;
- insurance;
- sales;
- transportation.

A steady increase in exposure also exists amongst professionals and the accommodation sector.

Number of Employees

In general, companies with a large number of employees, or that interact with a large number of customers, are particularly at risk. Employees who carry mobile devices, such as laptop computers and USB flash drives containing sensitive information, represent the most significant threat, accounting for almost half of all data breach incidents reported in data breach study conducted in the United States in 2007.⁹ Industries that use credit or debit card processing, and that access financial or health information, are at greater risk.

⁶ Supra, note 1.

⁷ Bill C-27, An Act to amend the Criminal Code (Identity theft and related misconduct) 2nd Sess., 39th Parl., 2007.

⁸ Supra, note 1.

⁹ Ponemon Institute, LLC, 2007 Annual Study: U.S. Cost of a Data Breach (PGP Corporation and Vontu Inc., November 2007).

High-Profile Companies

Furthermore, businesses with high public profiles are more susceptible to organized crime for financial profit or risk of terrorist activity. Although targeted criminal attacks pose a significant and growing exposure, it is important to note that internal breaches resulting, in most cases, from human error and not malicious action, constitute the greatest threat.¹⁰

Third Party Involvement

Companies that share personal information with third parties, such as outsourcers, contractors, consultants, and business partners, are at higher risk of a breach. Statistics show such breaches to be more costly than a breach by the company itself—averaging \$231 per compromised data record where third parties are involved as compared with \$171 otherwise.¹¹

International Aspects

Companies with global operations or that simply transmit personal information across borders are subject to unique risks as a result of their exposure to laws in foreign jurisdictions. Service agreements and contracts with customers in the United States typically obligate Canadian companies to comply with U.S. security and privacy regulations. Compliance with foreign laws may also place a Canadian business in a position of non-compliance with Canadian privacy laws. For example, Lakehead University in Thunder Bay, Ontario, caused a backlash in early 2008 when it elected to replace an outdated computer system with Google's service. Using U.S.-based Google's software system will force users into compliance with the U.S. Patriot Act, which was passed in the wake of the September 2001 terrorist attacks and which gives U.S. authorities sweeping powers to secretly view personal data held by U.S. organizations. The move outraged Lakehead's faculty association, which filed a grievance against Lakehead's administration and which is still in arbitration. They allege a breach of the collective agreement giving members a right to private communications.

Losses Associated with a Privacy Breach

Third-Party Liability

Losses that a company may incur as a result of harm to individuals or entities include the following:

- Compensation to clients or employees for general damages and out-of-pocket costs such as
 - loss from bank or credit card accounts;
 - general damages for inconvenience and violation of privacy rights;
 - economic loss arising from time off work spent dealing with the incident;
 - compensatory damages for emotional harm, humiliation, or embarrassment;
 - costs incurred in gathering information about breached data;
 - funds expended in protecting personal information such as changing credit and debit accounts;
 - cards and personal identifiers (such as Social Insurance Numbers), monitoring bank accounts, and credit card statements.
- Contractual fines/penalties: payment of fines and penalties arising out of a breach of contractually imposed industry-specific privacy standards, such as the Payment Card Industry Data Security Standard.¹²
- Subrogation: compensation to third parties such as downstream businesses or credit card companies that incur losses associated with a breach, including issuing new cards and paying fraud expenses associated with compromised cards, and then claiming reimbursement from the company sustaining the breach.

¹⁰ *Supra*, note 1.

¹¹ *Ibid*.

- Shareholder litigation: direct or derivative actions against the company and/or its board of directors to recover economic losses associated with any drop in share price that results from a breach.
- Defence: any legal costs incurred in responding to complaints and litigation, including class actions.

Regulatory/Law Enforcement Costs

Companies can expect to sustain significant losses associated with Canadian regulatory and other law enforcement agencies in connection with an actual or potential privacy breach including

- Canadian privacy commissioner: costs associated with self-reporting breaches, responding to complaints, and defending investigations and proceedings before the commissioner, including
 - legal defence costs;
 - compliance with regulator’s recommendations—including improvement to safety practices and retention of a third-party auditor.
- Federal Court: costs of proceedings associated with appeal of privacy commissioner’s findings, including damage awards for humiliation (with no cap on damage amount), fines, and penalties.
- Criminal Code of Canada:¹³ costs of defending criminal prosecutions, including legal costs, penal sanctions, and restitution awards.

First-Party/Direct Damages to Business

Losses that a company may incur as a result of harm to itself sustained from a breach include those related to

- A Response Plan
 - Discovery/detection: costs associated with the detection or discovery of the breach;
 - Reporting: costs incurred in reporting the breach to all appropriate internal and regulatory personnel/bodies;
 - Notification: costs incurred by the company to notify affected individuals with a letter, telephone call, email, or general notice that personal information was lost or stolen.
- Mitigation/Crisis Management: costs to help victims of the breach obtain information as to how to respond to the breach and minimize harm, including
 - credit report monitoring;
 - reissuance of new cards or accounts;
 - call centre and Web site to register complaints, provide information, and monitor activity;
 - public relations.
- Restoration/Reconstruction:
 - costs to restore lost or damaged information, including damaged IT systems;
 - changes to internal processes.
- Decline in Revenue: lost business related to loss of trust and confidence by customers, negative reputational effects, and any interruption to business services.

Risk Management

Given the potentially devastating effect of data and privacy breaches, boards of directors, general counsel, risk managers, finance departments, and technology leaders are recognizing this expanding area of risk and their obligation to mitigate through increased security, contractual

¹² PCI Security Standards Council <https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml>.

¹³ R.S.C. 1985, c. C-46.

provisions with service providers and vendors, and appropriate levels of insurance. In the process, they are finding that

- most organizations face exposure;
- most traditional insurance policies do not cover these risks;
- a privacy breach can have a significant impact on brand and reputation;
- no system can be designed to eliminate all of the potential for loss, as people and process failures cannot be eliminated and insiders may be perpetrators;
- many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond effectively.

Steps To Mitigate Risk

Mitigation of risk can be addressed through the steps outlined below:

1. Identification and understanding of risks and adoption of security measures: Mitigation of risk must start with an identification of a company's business risks, understanding the exposures, review of technical and information security policy safeguards, and alignment of company processes and protocols with relevant laws. An appropriate action plan should include the establishment of an effective privacy policy, disaster recovery and business continuity plans, mobile device protocols, employee training, and data classification standards.
2. Contractual indemnity: Companies that retain third-party service providers to perform services that allow access to the entities' electronic systems or data may well include contractual provisions in the service agreement that mandates that the service provider indemnify the entity for all losses arising from the loss or theft of personal information. Increasingly common is the push by entities to contractually require the service provider to purchase appropriate insurance coverage and that the company should have the opportunity to review or approve such coverage.
3. Insurance Coverage: An audit of a company's existing insurance program to determine coverage and gaps is an essential part of risk management due diligence. With the development over the past decade of new or unexpected privacy risks, traditional insurance products may not be able to respond adequately, with the result that the company in breach may be left wholly or partially exposed.

Traditional Insurance Response

Traditional insurance policies evolved at a time when today's technological risks were not envisioned and, as a result, most policies do not cover the risks that arise from privacy breaches. For example, whereas 10 or 15 years ago the risk associated with the theft of a laptop computer was the dollar value of that computer, today the relative value of the lost hardware is not great, but the value of the data on it may be enormous. The complexity of understanding and evaluating insurance programs and coverage options has resulted in the increased involvement of corporate in-house counsel in reviewing such options.

Property Insurance Policy

Property policies were designed for physical assets and physical perils and thus usually require physical damage to tangible property to trigger coverage. This is problematic because these policies typically exclude "data" from the meaning of tangible property. "Data" is often defined to mean representations of information or concepts in any form. Further, coverage is not triggered in privacy breaches because the damage to data is often caused by an electronic risk and not by a named physical peril, such as fire or wind. Excluded "data problems" are typically described as

- erasure, destruction, corruption, misappropriation, or misinterpretation of "data";
- error in creating, amending, entering, deleting, or using "data";
- inability to receive, transmit, or use "data".

Although losses caused directly or indirectly by a “data problem” are usually excluded, the resulting physical loss from a data problem may be covered if the further loss falls under an insured named peril. For example, damage to computer hardware arising from a fire may be covered although the loss of data information would not be covered. Since computer viruses and hacker attacks seldom damage systems physically, there is little coverage available. Furthermore, most property policies include computer virus exclusions, or provide for small sub-limits of coverage. Finally, these policies are not likely to cover reimbursement of first-party costs to mitigate the loss and manage the crisis.

Crime Insurance

Crime policies require an intent to harm, and cover theft of money, securities, and tangible property, but do not cover the true costs arising from the theft of data, information, or account numbers.

General Liability Insurance Policy (CGL)

CGL policies would not typically be triggered by a privacy breach, as the required trigger of physical damage to tangible property or bodily injury does not often occur in a privacy breach.

First, tangible property often specifically excludes “electronic data”, which is typically very broadly defined and includes such matters as information stored on computer software.

Second, coverage for “personal injury” is generally limited to oral and written publication of confidential information. Since hacking and other unauthorized disclosures of personal information do not involve any sort of intentional publication by the insured, there may be no coverage.

Third, there may be a gap related to emotional distress coverage. Many CGL policies only cover emotional stress resulting from bodily injury. Embarrassment and mental distress damages arising from a privacy breach will not typically result from an underlying physical injury.

Fourth, “advertising injury” coverage does not generally cover activities where the insured’s products or services are not being promoted. With the evolution of Web sites, electronic chat rooms, bulletin boards, and blogs that provide information beyond advertising, not all content may be covered.

Finally, similar to property insurance, CGL policies are unlikely to provide any first-party coverage for breach notification and crisis management.

Directors and Officers (D & O) Insurance Policy

D & O insurance policies generally only cover the entity’s directors and officers. Privacy breaches typically arise out of activities of the entity, and, under D & O insurance, the entity, if covered at all, would only have securities loss coverage. Furthermore, problematic exclusions would include those relating to property damage, intentional acts, and actions by one insured against another insured. Some coverage may be available in respect of actions against the board of directors arising from a drop in the value of the company’s stock that results from a privacy breach, or for employment practice liability arising out of an action by an employee for invasion of privacy.

Professional Liability and Media Policies

Errors and Omissions (E & O) policies, also referred to as professional liability policies, are intended to cover loss to third parties caused by errors, omissions, or negligent acts of the insured. The coverage is typically for economic damages only that arise out of a covered

professional service. Thus, loss arising out of negligence—for example, in leaving a laptop computer or network unsecured—would be excluded.

Media policies are a type of E & O coverage specially designed to cover risks of publishers, broadcasters, and other media-related entities. Such policies typically cover intellectual property risks such as defamation and copyright infringement, as well as invasion of privacy. Potential gaps in these types of coverage arise from exclusions relating to intentional acts, property damage, personal injury, and failure to cover losses to the insured itself, such as expenses to mitigate reputational damage.

Privacy and Network Security Insurance: An Innovative Insurance Response

The insurance market has been increasingly responsive to evolving privacy liability. Specially designed products that clarify the intent of coverage to respond to intangible assets such as codes, database records, and other electronic records, and providing dedicated coverage, responding particularly to the third-party risks, and first-party breach notification and crisis management expenses are emerging. These products often contain coverage for broader electronic breaches due to network security breaches, beyond breaches of personal information requirements. Other products that add extensions to traditional coverage have also emerged.

It is important to note that none of these products are standardized and a careful analysis of their terms is essential to ensure a full understanding of what coverage is being provided to the company. Flexibility in coverage to respond to the diversity of risks is essential, and thus working with an insurer to craft unique and customized coverage that will be responsive to a business' specific risks is important.

One of the newest products to emerge is the Privacy and Network Security Liability Policy, (see, Sample Privacy Network Policy, in Schedule B – attached). Highlights of this coverage may include the following:

Who is Covered?

Typically coverage is provided for the organization, its subsidiaries, directors, officers, trustees, employees, and independent contractors for whom the insured is liable.

How is the Coverage Triggered?

The policy is typically triggered by notice of a “claim”, which often includes a written demand for monetary or non-monetary damages, civil or criminal proceedings, or administrative or regulatory investigations or proceedings.

In Canada, where breach notification is not yet mandated (unlike in the United States), it is important that the policy contain a trigger that is less restrictive than that contained in many U.S. policies. Thus, it is desirable to have the first-party coverage triggered when the insured reports a potential privacy breach, as opposed to waiting for an actual breach to occur.

What is Covered?

- **Privacy liability:** These policies may cover third-party damages and claim expenses that arise out of unauthorized access to, collection of, and use or disclosure of personal information and that results in harm to employees or third parties. This would include losses arising from intentional hacking by rogue employees or third parties, or by negligence. The personal information may be in any format, including paper. The coverage usually includes amounts the insured is legally obligated to pay as a result of the breach, including defence expenses as a result of a regulatory or criminal investigation or prosecution. Broader types of policies may provide coverage for civil penalties or sanctions imposed by a regulatory body.

- Crisis management and notification expenses: The policy will usually provide coverage for expenses incurred in attempting to mitigate reputational damage as a result of a privacy breach, including retention of public relations firms and crisis management costs such as
 - call centre and Web site expenses to handle inquiries from employees or customers;
 - credit monitoring;
 - costs involved in notifying customers or employees whose data have been compromised.
- Network security liability: The policy will typically provide coverage for third-party damages and defence expenses that arise from an unauthorized access or use of computer data, theft of data, denial of network service, or malicious code. Additional damages, typically referred to as contingent business interruption losses, which are caused downstream by network outages or the transmission of malicious codes or viruses from the insured to a third party (such as a service provider) may also be covered.

What is Excluded?

Given the differing wordings between insurance companies, it is impossible to provide a complete listing of policy exclusions. As noted previously, a thorough review of the policy with keen attention to detail is key to obtaining appropriate coverage.

A general overview of some standard exclusions includes the following:

- Losses covered under other policies, such as pollution exposure, director and officer claims, bodily injury, property damage, and employment practice claims;
- Conduct exclusions, such as fraudulent conduct, illegal profit, intentional violation of law;
- Underwriting exclusions, such as litigation that is pending prior to the policy inception, claims where notice was provided for a past policy, contractual obligations, and claims where one insured is claiming against another insured.

Limits and Capacity

Worldwide capacity approaching \$200 million per policy purchased is available for a multi-layered insurance program. Carriers that place primary policies typically offer limits between \$5 million and \$20 million for the first layer, with an average limit of \$10 million. Most carriers offer a lower (sub-limit) for first-party coverage related to privacy breaches.

Underwriting

Historically, companies that wished to purchase coverage for electronic risks purchased a cyber insurance policy

—a time consuming and expensive exercise that often involved the completion of lengthy, highly technical applications, and committing to extensive third-party security audits (often prior to the policy inception and at the insured's own expense). These onerous hurdles have largely been eliminated by some of the newer privacy policies.

Today, companies may be required to fill out an application, which can be as short as four pages, and may be required to undergo a post-binding audit at the insurer's expense. The audit may be a useful due diligence check of a company's IT security and protocols, and does not affect the policy terms or pricing. (see, Sample Privacy Policy Application, in Schedule C – attached) Privacy underwriters largely define a company's privacy risk by taking into consideration the following:

- Company revenue;
- Applicability of and compliance with relevant privacy laws;
- Number of employees;
- Interaction with a large number of individual customers;
- Type and sensitivity of information collected;
- Length of time information is stored and for what purpose;

- Obligations/commitments made by the company regarding protection, retention, notification;
- Whether the company has a large public profile (i.e., whether it would be on the radar screen of criminal hackers);
- Network security procedures and compliance, including encryption and mobile device protections;
- History of claims or breaches.

With the frequency and severity of privacy breaches on the uphill trajectory, and with more stringent breach notification likely to be statutorily mandated in Canada before year's end, it is anticipated that significant privacy losses loom on the horizon. Many companies are unlikely to be able to avoid risk altogether, particularly when one considers that the majority of losses currently arise from innocent mistakes by employees, such as the loss of a laptop computer through theft or negligence. Even the best of security protections may not be enough to avoid all losses. With the significant advances in insurance designed to respond to today's expanding exposures to privacy breaches, a prudent risk management approach must entail the careful consideration of all available risk transfer solutions.

This chapter is intended to provide an overview of privacy liability and insurance for general and illustrative purposes only. The material presented is not a complete or exhaustive analysis of legal liability exposures or risks, nor of privacy liability insurance coverage. The terms of privacy liability insurance are not standardized. The availability of insurance coverage to respond to any particular claim will depend on the specific facts and circumstances of the claim and the language of the policy issued. Advice with respect to particular insurance needs or actual or potential legal liability must be obtained from an insurance broker or lawyer, respectively.

SCHEDULE A

Map of Canadian Privacy Laws

NYMITY's Map of Privacy Laws

Privacy Commissioners in Canada

British Columbia

David Loukidelis
Information and Privacy
Commissioner for
British Columbia
(250) 387-5629
www.oipc.bc.ca

Prince Edward Island

Rebecca Wellner
Information and Privacy
Commissioner of
Prince Edward Island
(902) 368-4099
www.gov.pe.ca

Alberta

Franklin Work
Information and Privacy
Commissioner of Alberta
(780) 422-6860
www.oipc.ab.ca

Nova Scotia

Dulcie McCallum
Freedom of Information
and Privacy Review Office
(902) 424-4684
www.foipop.ns.ca

Saskatchewan

Gary Dickson, Q.C.
Information and Privacy
Commissioner of
Saskatchewan
(306) 787-8350
www.oipc.sk.ca

Newfoundland

Phil Wall
Information and Privacy
Commissioner
(709) 729 6309
www.oipc.gov.nl.ca/

Manitoba

Irene Hamilton
Ombudsman
Office of the Ombudsman
(204) 982-9130
www.ombudsman.mb.ca

Yukon

Hank Moorlag
Ombudsman and
Information and Privacy
Commissioner of the Yukon
(867) 667-8468
www.ombudsman.yk.ca

Ontario

Ann Cavoukian Ph.D
Information and
Privacy Commissioner
of Ontario
(416) 326-3333
www.ipc.on.ca

Northwest Territories

Elaine Keenan-Bengts
Information and Privacy
Commissioner of the
Northwest Territories
(867) 669-0976

Quebec

Me Jacques Saint-Laurent
President Commission
d'accès à l'information
du Québec
(418) 528-7741
www.cai.gouv.qc.ca

Nunavut

Elaine Keenan-Bengts
Information and Privacy
Commissioner of Nunavut
(867) 669-0976
http://www.info-
privacy.nu.ca/en/home

New Brunswick

Bernard Richard
Ombudsman
Province of New
Brunswick
(506) 453-2789
www.gnb.ca/0073/index-e.asp



Produced by:

NYMITY

SIMPLE SOLUTIONS FOR CONTROLLING PRIVACY RISKS

www.nymity.com

Sponsors



Chartered Accountants of Canada / Comptables agréés du Canada



Lang Michener LLP
Lawyers - Patent & Trade Mark Agents



CANADIAN MARKETING ASSOCIATION / CMA



RCC
Retail Council of Canada



FASKEN MARTINEAU



BAKER & MCKENZIE
BARRISTERS & SOLICITORS



CANADIAN STANDARDS ASSOCIATION



THOMSON
CARSWELL



iapp
international association of privacy professionals



QMI
Management System Integration

Federal Privacy Acts



Jennifer Stoddart

Privacy Commissioner of Canada
1-800-282-1376 • www.privcom.gc.ca

*PIPEDA - Personal Information Protection and Electronic Documents Act

Note:

1. Federal works, undertakings and businesses are exclusively subject to PIPEDA, regardless of location in Canada.
2. PIPEDA applies to all federal and provincial cross-border transfers of personal information in a commercial activity

SCHEDULE B

Sample Privacy Network Policy



Privacy and Network Liability Insurance

Effectuated with certain Lloyd's Underwriters (hereinafter called the "Underwriter") throughout

Lloyd's Approved Coverholder ("the Coverholder"):
Executive Risk Insurance Services Ltd.
365 Bay Street, 12th Floor
Toronto, Ontario, M5H 2V1 Canada



DECLARATIONS

PRIVACY AND NETWORK LIABILITY INSURANCE POLICY

THIS IS A **CLAIMS** MADE POLICY. EXCEPT AS OTHERWISE PROVIDED, THIS POLICY COVERS ONLY **CLAIMS** FIRST MADE TO THE **UNDERWRITER** DURING THE **POLICY PERIOD** OR ANY **EXTENDED REPORTING PERIOD**. TERMS THAT APPEAR IN BOLD FACE TYPE HAVE SPECIAL MEANINGS. SEE THE DEFINITIONS FOR MORE INFORMATION. PLEASE READ THIS POLICY CAREFULLY.

These Declarations along with the completed and signed **Application** and the Policy with endorsements shall constitute the entire contract between the **Insureds** and the **Underwriter**.

Policy No.: _____ Renewal of Policy No.: _____

Item 1. Insured Organization:

Principal Address:

Item 2. Policy Period:

From: _____ To: _____

Both days at 12:01 a.m. Local Time at the Principal Address stated in Item 1.

Item 3. Limit of Liability: A. \$ () CAD aggregate limit of liability
(Aggregate for all Insuring Agreements combined including **Claim Expenses**)
B. \$ () CAD limit of liability for Insuring Agreements

INSURING AGREEMENTS	LIMIT OF LIABILITY INCLUDES CLAIM EXPENSES
A. Privacy Liability	CDN each Claim/and in aggregate
B. Crisis Management and Notification Expenses	CDN each Claim/ and in aggregate
C. Network Security Liability	CDN each Claim/and in aggregate

Item 4. Retention (including Claims Expenses):
\$() CAD each **Claim** under Insuring Clause A
\$() CAD each **Claim** under Insuring Clause B
\$() CAD each **Claim** under Insuring Clause C

Item 5. Retroactive Date:

Item 6. Pending and Prior Litigation Date:

Item 7. Optional Extended Reporting Period: 100% of annual premium

Item 8. Premium: \$() CAD Brokerage Commission Paid: () %

Item 9. NOTICE pursuant to Clause 10, shall be given to:

Attention: Claims Department
Executive Risk Insurance Services Ltd.
365 Bay Street, 12th Floor
Toronto ON M5H 2V1

Tel: 416-979-3600 Fax: 416-979-8337
Email: claims@execurisk.com

Issued and dated in Toronto:

The Policy consists of this Declarations page as well as the **Application** and all endorsements that are attached hereto.

IDENTIFICATION OF UNDERWRITER / ACTION AGAINST UNDERWRITER

This Policy has been effected in accordance with the authorization granted to the Coverholder by the Underwriting Members of the Syndicates whose definitive numbers and proportions are shown in the Table attached to Agreement No. N34327 (hereinafter referred to as "the **Underwriters**"). The **Underwriters** shall be liable hereunder each for his own part and not one for another in proportion to the several sums that each of them has subscribed to the said Agreement.

In any action to enforce the obligations of the **Underwriters** they can be designated or named as "Lloyd's Underwriters" and such designation shall be binding on the **Underwriters** as if they had each been individually named as defendant. Service of such proceedings may validly be made upon the **Attorney In Fact** in Canada for Lloyd's Underwriters, whose address for such service is 1155 rue Metcalfe, Suite 2220, Montreal, Quebec H3B 2V6.

NOTICE

Any notice to the **Underwriters** may be validly given to the Coverholder.

In witness whereof this policy has been signed as authorized by the **Underwriters**, by Executive Risk Insurance Services Ltd.

Per

The **Insured** is requested to read this Policy, and if incorrect, return it immediately for alteration.

All inquiries and disputes with respect to this Policy are to be addressed to this Coverholder.

THIS POLICY CONTAINS CLAUSES WHICH MAY LIMIT THE AMOUNT PAYABLE.



In consideration of payment of the premium and reliance upon the statements in the **Application** which is made a part of and attached to this Insurance Policy (hereinafter referred to as the "Policy") and subject to the Declarations and the terms and conditions of this Policy, the **Insureds** and the **Underwriter** agree as follows:

1. INSURING AGREEMENTS

A. *PRIVACY LIABILITY*

The **Underwriter** shall pay on behalf of the **Insured** those amounts, which the **Insured** is legally obligated to pay as **Loss** resulting from a **Claim** first made against any **Insured** during the **Policy Period**, or if exercised during the **Extended Reporting Period** for any **Wrongful Acts** committed, attempted, or allegedly committed or attempted, on or after the **Retroactive Date** set forth in Item 5 of the Declarations.

B. *CRISIS MANAGEMENT EXPENSES AND NOTIFICATION EXPENSES*

The **Underwriter** will pay **Crisis Management Expenses** and **Notification Expenses** incurred by the **Insured** arising from a **Claim** first made against any **Insured** during the **Policy Period** or **Extended Reporting Period** resulting from a **Wrongful Act** committed, attempted, or allegedly committed or attempted on or after the **Retroactive Date** set forth in Item 5 of the Declarations.

C. *NETWORK SECURITY LIABILITY*

The **Underwriter** shall pay on behalf of the **Insured** those amounts, which the **Insured** is legally obligated to pay as **Loss** arising from a **Claim** first made against any **Insured** during the **Policy Period** or **Extended Reporting Period** resulting from a **Wrongful Act** committed, attempted, or allegedly committed or attempted on or after the **Retroactive Date** set forth in Item 5 of the Declarations.

2. ESTATES, LEGAL REPRESENTATIVES AND SPOUSES

Subject otherwise to the terms and conditions of this Policy, coverage shall extend to **Claims** for the **Wrongful Acts** of **Insured Persons** made against the estate, heir, legal representative, or assign of any **Insured Person** who is deceased, or against the legal representative or assign of **Insured Persons** who are incompetent, insolvent or bankrupt, or, against the spouse of an **Insured Person**, for such spouse's ownership interest in marital property which the claimant seeks as recovery. No coverage is provided for any **Wrongful Act** of any estate, heir, legal representative, assign or spouse.

3. DEFENCE AND SETTLEMENT

The **Underwriter** shall have the right and duty to defend any covered **Claim**, even if such **Claim** is groundless, false, or fraudulent. The **Underwriter's** duty to defend shall cease upon exhaustion of the applicable Limits of Liability. The **Insured** shall have the right, but not the duty, to appoint counsel to defend the **Claim**, subject to the prior written consent of the **Underwriter**, which shall not be unreasonably withheld. **Claim Expenses** incurred by the **Underwriter**, or by the **Insured** with the written consent of the **Underwriter**, are part of and not in addition to the **Underwriter's** applicable Limit of Liability set forth in Item 3B of the Declarations. Payment by the **Underwriter** of **Claim Expenses** reduces and may completely exhaust such applicable Limit of Liability. **Loss** shall be applied against the retention payable by the **Insured**.

The **Insured** shall not admit liability, make any payment, assume any obligations, incur any expense, enter into any settlement, stipulate to any judgment or award or dispose of any **Claim** without the **Underwriter's** written consent, which shall not be unreasonably withheld, unless otherwise provided under this Clause 3.

The **Underwriter** agrees that the **Insured** may settle any **Claim** where the **Loss** does not exceed 50% of the Retention, provided the entire **Claim** is resolved and the **Insured** receives a full release from all claimants, or court approval of the settlement, and notice of such settlement is provided to the **Underwriter**. This clause shall not apply where any dispute exists between the **Underwriter** and the **Insured** over whether certain **Claims** have arisen due to **Interrelated Wrongful Acts**.

Solely with respect to Insuring Agreement B, the **Insured** may incur **Notification Expenses** and/or **Crisis Management Expenses** arising from a **Claim** without the **Underwriter's** prior written consent, provided notice of the intent to incur such expenses, and any known details of same, is provided to the **Underwriter** as soon as practicable.

If the **Insured** refuses to consent to a settlement recommended by the **Underwriter** and acceptable to the claimant and elects to contest the **Claim**, the **Underwriter's** liability for any **Loss** shall not exceed the amount for which the **Claim** could have been settled, plus the **Claim Expenses** incurred to the date of such refusal, and the **Underwriter** shall have the right to withdraw from the further defence thereof by tendering control of said defence to the **Insured**. This clause shall not apply to any settlement where the total incurred **Loss** does not exceed all applicable retentions.

4. ALLOCATION

If **Loss** covered by this Policy and loss not covered by this Policy are incurred, either because a **Claim** includes both covered and uncovered matters or because a **Claim** is made against both an **Insured** and others, the **Insured** and the **Underwriter** shall use their best efforts to agree upon a fair and proper allocation based upon relative legal and financial exposures of such amount between covered **Loss** and uncovered loss.

If the **Insureds** and the **Underwriter** agree on an allocation of **Claim Expenses**, the **Underwriter** shall advance on a current basis **Claim Expenses** allocated to the covered **Loss**. If the **Insureds** and the **Underwriter** cannot agree on an allocation:

- (a) no presumption as to allocation shall exist in any arbitration, litigation or other proceeding;
- (b) the **Underwriter** shall advance on a current basis **Claim Expenses** which the **Underwriter** believes to be covered under this Policy until a different allocation is negotiated, arbitrated or judicially determined; and
- (c) the **Underwriter**, if requested by the **Insured**, shall submit the dispute to binding arbitration. The arbitration panel shall consist of three arbitrators, one chosen by each of the **Insured** and the **Underwriter** and the third selected by the first two arbitrators, or on any other terms which the **Underwriter** and **Insured** agree upon.

Any negotiated, arbitrated or judicially determined allocation of **Claim Expenses** on account of a **Claim** shall be applied retroactively to all **Claim Expenses** on account of such **Claim**, notwithstanding any prior advancement to the contrary. Any allocation or advancement of **Claim Expenses** on account of a **Claim** shall not apply to or create any presumption with respect to the allocation of other **Loss** on account of such **Claim**.

5. ASSISTANCE, COOPERATION AND SUBROGATION

The **Insureds** agree to provide the **Underwriter** with all information, assistance and cooperation which the **Underwriter** reasonably requests in the defence of any **Claim** and in enforcing any right of subrogation,

contribution or indemnity. The **Insureds** agree that in the event of a **Claim** they will do nothing that may prejudice the **Underwriter's** position or its potential or actual rights of recovery.

6. EXCLUSIONS

The **Underwriter** shall not be liable for **Loss** on account of any **Claim**:

- a) based upon, arising out of or related to any circumstance if written notice of such circumstance has been given under any policy of which this Policy is a replacement or renewal.
- b) based upon, arising out of or related to any demand, litigation, formal investigation, administrative, regulatory or other proceeding pending, or order or judgment entered against any **Insured** on or prior to the **Pending and Prior Litigation Date** specified in Item 6 of the Declarations, or alleging or derived from the same or substantially the same facts underlying or alleged therein.
- c) made against any **Insured Person**:
 - (i) based upon, arising out of or related to any deliberately fraudulent, criminal, dishonest or malicious act, error or omission, or any intentional or knowing violation of any law, by any such **Insured Person**, however this exclusion shall not apply in circumstances where the **Insured Person's** intentional or knowing violation of any law is required by or imposed on the **Insured Person** by operation of law, whether the law be legislative, or by court order, judgment or decree; or
 - (ii) based upon, arising out of or related to such **Insured Person** having gained any profit, remuneration or other advantage to which such **Insured Person** was not legally entitled

if a final judgment, final adjudication, binding arbitration decision, or written admission under oath by such **Insured Person** in any proceeding establishes such conduct by the **Insured Person**. At such time, the **Insured Person** shall reimburse the **Underwriter** for all **Claim Expenses** incurred on behalf of such **Insured Person** and the **Underwriter** shall have no further liability for **Claims Expenses** in connection with such **Insured Person**.

- d) made against any **Insured Organization** or **Subsidiary**:
 - (i) based upon, arising out of or related to any deliberately fraudulent, criminal, dishonest or malicious act, error or omission, or any intentional or knowing violation of any law, , by any **Insured Person** only where more than one of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Technology Officer, Chief Privacy Officer or Chief Information Officer, (or any equivalent positions) and any Director, participated in or were in collusion with such **Insured Person's** conduct; or
 - (ii) based upon, arising out of or related to any **Insured Person** having gained any profit, remuneration or other advantage to which such **Insured Person** was not legally entitled only where more than one of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Privacy Officer, Chief Technology Officer, Chief Information Officer (or any equivalent positions) and any Director, participated in or were in collusion with such **Insured Person**

if a final judgment, final adjudication, binding arbitration decision, or written admission under oath by such Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Technology Officer, Chief Privacy Officer or Chief Information Officer (or any equivalent positions) and any Director who participated in or were in collusion with such **Insured Person**, in any proceeding, establishes such conduct. At such time, the **Insured** shall reimburse the **Underwriter** for all **Claim Expenses** incurred on behalf of the **Insured** and the **Underwriter** shall have no further liability for **Claims Expenses** in connection with the **Insured**. However this exclusion shall not apply in circumstances where the **Insured Person's** intentional or knowing violation of any law is required by

or imposed on the **Insured Person** by operation of law, whether the law be legislative, or by court order, judgment or decree;

- e) Brought or maintained by or on behalf of any other **Insured**, or any other natural person or entity for whom or which an **Insured** is legally liable except :
 - (i) for **Wrongful Acts** expressly covered under Insuring Agreement A; or
 - (ii) a **Claim** brought or maintained by an **Insured** for contribution or indemnity, if the **Claim** directly results from another **Claim** covered under this Policy;
- f) for bodily injury, sickness, disease or death of any person, or physical damage to or loss or destruction of any tangible property including loss of use thereof. However bodily injury shall not include mental anguish, emotional distress, or humiliation. Data is not considered tangible property;
- g) based upon, arising out of or related to the **Insured's** employment practices, including but not limited to wrongful termination, sexual harassment, employment-related libel, slander or defamation, or any discrimination of any kind;
- h) based upon, arising out of or related to satellite failures, electrical or mechanical failures and/or interruption, including but not limited to electrical disturbance, spike, brownout or blackout, and outages to gas, water, telephone, cable, telecommunications or other infrastructure, unless such infrastructure is under the **Insured's** operational control;
- i) based upon, arising out of or related to:
 - (i) the rendering or failure of an **Insured** to render professional services including any negligence in the performance of an **Insured's** professional services; or
 - (ii) the failure, breakdown, or injury resulting from any actual or alleged defects in goods or products which an **Insured** commercially manufactures, supplies, sells, distributes or markets, including work performed by an **Insured** to repair, alter, maintain or install goods or products for commercial purpose in the course of its business, including the breach of any warranties or representations with respect to the goods or products of an **Insured** that meet this description; or
 - (iii) an **Insured's** failure to properly perform the work or services for which it is typically hired or retained;
- j) for any fees, expenses or costs paid to or charged by the **Insured**;
- k) for breach of any express, implied, actual or constructive contract, warranty, guarantee or promise, unless such liability would have attached to the **Insured** even in the absence of such contract, warranty, guarantee or promise. However, this exclusion shall not apply to a breach of the **Insured's** own privacy statement or of any agreement, warranty, guarantee or promise, by the **Insured** to keep personal information private, or to hold harmless or indemnify any person for breach of same;
- l) based upon, arising out of or related to any of the following:
 - (i) presence of pollutants or contamination of any kind.; or
 - (ii) actual, alleged or threatened discharge, dispersal, release, or escape of pollutants or contamination of any kind; or
 - (iii) direction or request to test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize pollutants or in any way respond to or assess the effects of pollutants or contamination of any kind; or
 - (iv) manufacturing, mining, use, sale, installation, removal, distribution of or exposure to asbestos, materials, or products containing asbestos, asbestos fibers or dust; or
 - (v) Ionizing radiation or contamination by radioactivity from any nuclear fuel or any nuclear waste from the combustion of nuclear fuel; or
 - (vi) actual, potential or alleged presence of mold, mildew or fungi of any kind whatsoever; or
 - (vii) radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or

- nuclear component thereof; or
- (viii) the existence, emission or discharge of any electromagnetic field, electromagnetic radiation; or electromagnetism that actually or allegedly affects the health, safety or condition of any person or the environment or that affects the value, marketability, condition or use of any property;

For the purposes of this exclusion contamination shall not include **Malicious Code**.

- m) based upon, arising out of or related to any of the following:
- (i) purchase, sale, offer of or solicitation of an offer to purchase or sell securities, or violation of any securities law;
 - (ii) racketeering or money laundering;
 - (iii) anti-trust violations, restraint of trade or unfair competition;
 - (iv) violation of the responsibilities, obligations or duties imposed upon fiduciaries of employee benefit plans;
 - (v) based upon, arising out of or related to the validity, invalidity, infringement, violation, or misappropriation of intellectual property rights, licensing statutes or regulations including but not limited to patent, trade secrets, copyright, and trademark;
- n) based upon, arising out of or related to fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, an act of God or any other physical event however caused;
- o) based upon, arising out of or related to any strike, lockout or similar labour action, acts of terrorism, war, invasion, acts of foreign enemy, hostilities, war like operation(whether declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to a popular uprising, military or usurped power. **Malicious Code** shall not, in any circumstance, be considered an act of terrorism;
- p) based upon, arising out of or related to any trading losses or trading liabilities, monetary value of any electronic fund transfers or transactions by or on behalf of the **Insured** which is lost, diminished, or damaged during transfer from, into or between accounts, or the face value of coupons, price discounts, prizes, awards, or any other valuable consideration given in excess of the total contracted or expected amount.

7. SEVERABILITY OF EXCLUSIONS AND NOTICE REQUIREMENT

With respect to the Exclusions in subsection 6, no act, error or omission pertaining to or knowledge possessed by any **Insured** shall be imputed to any other **Insured**, unless otherwise provided under Exclusion 6 (d) to determine if coverage is available.

With respect to the notice requirements in subsection 10 of this Policy, no act, error or omission pertaining to or knowledge possessed by any **Insured Person** shall be imputed to any other **Insured Person**. However, with respect to the failure to give notice to the **Underwriter** as required under this Policy, any **Insured Person** entitled to the benefit of this severability section shall provide notice to the **Underwriter** in compliance with such notice condition promptly after obtaining knowledge of the failure by any other **Insured** to comply therewith, and the reporting of any such **Claim** must be made during the **Policy Period** or the **Extended Reporting Period**, if applicable.

LIMIT OF LIABILITY AND RETENTION

All **Claims** arising out of the same **Wrongful Act** and all **Interrelated Wrongful Acts** of any **Insured** shall be deemed one **Claim**, and such **Claim** shall be deemed to have originated in the earliest **Policy Period** in which a **Claim** is first made against any **Insured** alleging any such **Wrongful Act** or **Interrelated Wrongful Act**.

The **Underwriter's** maximum liability for each **Loss**, whether covered under one or more Insuring Agreement, shall be the Limit of Liability for each **Loss** set forth in Item 3(B) of the Declarations. The **Underwriter's** maximum aggregate liability for all **Loss** on account of all **Claims** first made during the **Policy Period** shall be as indicated in Item 3 (A) of the Declarations.

The Limit of Liability for the **Extended Reporting Period** shall be part of and not in addition to the Limit of Liability for the immediately preceding **Policy Period**.

If a single **Loss** is covered under more than one Insuring Agreement, the single highest applicable Limit of Liability set forth in Item 3 (B) of the Declarations shall be **Underwriter's** maximum liability in total for all of the applicable Insuring Agreements combined.

The **Underwriter's** liability under this Policy shall apply only to that part of each **Loss** which is excess of the Retention set forth in Item 4 of the Declarations and such Retention shall be borne by the **Insured** uninsured and at their own risk.

8. EXTENDED REPORTING PERIOD

A. Basic Extended Reporting Period: In the event of cancellation or non-renewal of this Policy by the **Insured** or by the **Underwriter**, other than for non-payment of premium, an **Extended Reporting Period** of thirty (30) days following such cancellation or non-renewal shall be automatically granted hereunder at no additional premium. Such **Extended Reporting Period** shall cover **Claims** first made during this thirty (30) day **Extended Reporting Period** but only in respect of any **Wrongful Act** committed prior to the date of cancellation or non-renewal. No **Claim** shall be accepted by the **Underwriter** in this thirty (30) day **Extended Reported Period** if the **Insured** is entitled to indemnity under any other insurance or would have been entitled to indemnity under such insurance but for the exhaustion thereof.

B. Optional Extended Reporting Period: In the event of cancellation or non-renewal of this Policy by the **Insured** or the **Underwriter**, other than for non-payment of premium, the **Insured** shall have the right, upon payment in full of 100% of the annual premium shown in Item 8 of the Declarations, within thirty (30) days from non-renewal or cancellation, to a twelve (12) month optional **Extended Reporting Period** from the cancellation or non-renewal date, but only in respect of any **Wrongful Act** committed prior to the date of cancellation or non-renewal. At the commencement of the optional **Extended Reporting Period**, the entire premium shall be deemed fully earned, and in the event the **Insured** terminates the optional **Extended Reporting Period** for whatever reason prior to its natural expiration, the **Underwriter** will not be liable to return any premium paid for the optional **Extended Reporting Period**.

The offer of different renewal terms and conditions or premiums shall not constitute non-renewal. All notices and premium payments with respect to the **Extended Reporting Period** shall be directed to the **Underwriter** through the entity named in the Item 1 of the Declarations.

9. REPORTING AND NOTICE

The **Insured** shall, as a condition precedent to exercising its rights under this Policy, give to the **Underwriter** written notice as soon as practicable upon any of the **Insured's** Risk Manager, General Counsel, director, Chief Technology Officer, or Chief Privacy Officer (or similar equivalent position), becoming aware of any **Claim** made against any **Insured** for a **Wrongful Act**.

If during the **Policy Period**, the **Insured** becomes aware of circumstances which could give rise to a **Claim**, and gives written notice of such to the **Underwriter**, then any **Claims** subsequently arising from such circumstances shall be considered to have been made during the **Policy Period** or the **Extended Reporting Period** in which the circumstances were first reported to the **Underwriter**.

The **Insured** shall, as a condition precedent to exercising its rights under this Policy, provide to the **Underwriter** such information and cooperation as it may reasonably require, including but not limited to a description of the **Claim**, relevant documents including system security and event logs, access to witnesses, the nature of the alleged or potential consequences and damages, the names of actual or potential claimants, and the manner in which the **Insured** first became aware of the **Claim** or circumstance.

10. OTHER INSURANCE

This Policy shall apply in excess of any other valid and collectible insurance available to the **Insured**, including any retention or deductible portion thereof, unless such other insurance is written only as specific excess insurance over the limits of liability of this Policy.

11. ACTION AGAINST UNDERWRITERS AND BANKRUPTCY

No action shall lie against the **Underwriter** or the **Underwriters'** representatives unless, as a condition precedent thereto there shall have been full compliance with all terms and conditions of this Policy. No person or organization shall have the right under this Policy to join the **Underwriter** or the **Underwriter's** representatives as a party to any action against the **Insured** to determine the **Insured's** liability. Bankruptcy or insolvency of an **Insured** or its estate shall not relieve the **Underwriter** of its obligations nor deprive the **Insured** of its rights hereunder.

12. MERGERS AND ACQUISITIONS

A. Newly Acquired Subsidiaries

During the **Policy Period**, if the **Insured Organization** or any of the **Subsidiaries** acquire another entity whose annual revenues are more than fifteen percent (15%) of the total revenues of the **Insured Organization's** as set forth in the most recent audited financial statements, then for a period of ninety (90) days after the effective date of the acquisition, the newly acquired **Subsidiary** will be included within the definition of the **Insured**, but only for **Wrongful Acts** committed or allegedly committed after the effective date of the acquisition. Upon expiration of the ninety (90) day period, there shall be no coverage under this policy for **Wrongful Acts** committed or allegedly committed by the newly acquired **Subsidiary** unless the **Insured** gives the **Underwriter** written notice of the acquisition containing full details thereof, and the **Underwriter** agrees to add coverage for the newly acquired **Subsidiary** upon such terms, conditions, and limitations of coverage and such additional premium as the Underwriter, in its sole discretion, may require.

B. Mergers or Consolidations

During the **Policy Period**, if the **Insured Organization** consolidates or merges with or is acquired by another entity, or sells substantially all of its assets to another entity, then all coverage under this Policy shall continue to the expiration of the **Policy Period** but only for **Wrongful Acts** that occurred prior to the date of the consolidation or merger.

Should an entity cease to be a **Subsidiary** before or after the inception date of this Policy, coverage with respect to such entity shall continue as if it was still a **Subsidiary**, but only with respect to a **Claim** that arises out of a **Wrongful Act** committed by that entity prior to the date that it ceased to be a **Subsidiary**.

C. ASSIGNMENT AND ALTERATION

The interest hereunder of any **Insured** is not assignable. The terms and conditions of this Policy shall not be waived or changed except by written endorsement to this Policy signed by the **Underwriting Manager** or **Underwriter**.

13. AUTHORIZATION CLAUSE

By acceptance of this Policy the **Insured Organization** agrees to act on behalf of all **Insureds** with respect to the giving of notice of a **Claim**, the giving or receiving of notice of cancellation or non-renewal, the payment of premiums, the receiving of any premiums that may become due under this Policy, the negotiation of endorsements, consenting to any settlement, exercising the right to the **Extended Reporting Period**, and the giving or receiving of any other notice provided for in this Policy, and all **Insureds** agree that the **Insured Organization** shall so act on their behalf.

14. REPRESENTATIONS AND SEVERABILITY

In granting coverage to any of the **Insureds**, the **Underwriter** has relied upon the declarations and statements in the **Application** for this Policy and upon any declarations and statements in the original written application submitted to any other Underwriter in respect of any prior coverage. All such declarations and statements are the basis of such coverage and shall be considered as incorporated in and constituting part of this Policy.

Such applications shall be construed as a separate application for coverage by each **Insured Person** and no statement in such application or knowledge possessed by any **Insured Person** shall be imputed to any other **Insured Person** for the purpose of determining if coverage is available. Statements in such application or knowledge possessed by any of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Technology Officer, Chief Privacy Officer, Chief Information Officer (or any equivalent positions) and any Director shall be imputed to the **Insured Organization** and any **Subsidiaries** for the purpose of determining coverage under this Policy.

15. CANCELLATION

This Policy may be cancelled by the **Insured**, by surrender thereof to the **Underwriter** or by mailing the **Underwriter** through the **Underwriting Manager**, written notice stating when the cancellation shall be effective. This Policy is non-cancellable by the **Underwriter** except for non-payment of premium when due, in which case cancellation shall be effected by the **Underwriter** mailing a written notice of cancellation to the **Insured** at the address shown in the Declarations stating when not less than ten (15) days thereafter, such cancellation shall be effective. Mailing of notice shall be sufficient proof of notice. The time of surrender or the effective date and hour of cancellation stated in the notice shall become the end of the policy period. Delivery (where permitted by law) of such written notice either by the **Insured** or by the **Underwriter** shall be equivalent of mailing.

If the **Insured** cancels this policy, the earned premium shall be computed in accordance with the Lloyd's short rate table and procedure, provided that the premium shall be deemed fully earned if any **Claim** has been notified to the **Underwriter** under this Policy. In that event, the **Underwriter** agrees that the Policy will not be cancelled midterm solely on the basis of any valid **Claim** notified to the **Underwriter**.

16. SERVICE OF SUIT

It is agreed that in the event of the failure of **Underwriters** to pay any amount claimed to be due hereunder, **Underwriters**, at the request of any person or entity insured hereunder will submit to the jurisdiction of any court of competent jurisdiction within the territorial jurisdiction of Canada and will comply with all requirements necessary to give such court jurisdiction. Nothing in this Clause constitutes or should be understood to constitute a waiver of **Underwriters'** rights to commence an action in any court of competent jurisdiction in the territorial jurisdiction of Canada, to remove an action commenced outside the territorial jurisdiction of Canada to a Canadian court, or to seek a transfer of an action commenced in one province or territory of Canada to a court in another province or territory as permitted by the laws of Canada or of any Canadian province. It is further agreed that service of process in such suit may be made upon the **Attorney in Fact**, and that in any suit instituted against the **Underwriters** they will abide by the final decision of such court or of any appellate court in the event of an appeal.

The **Attorney in Fact** is authorized and directed to accept service of process on behalf of **Underwriters** in any such suit and/or upon the request of any person or entity insured hereunder to give a written undertaking to such person or entity that they will enter a general appearance upon **Underwriters'** behalf in the event such a suit shall be instituted.

18. TERRITORY

This Policy applies to **Claims** made and acts as committed or alleged to have been committed anywhere in the world.

19. DEFINITIONS

- A. Application** means all applications, including any attachments thereto, and all other information and materials submitted by or on behalf of the **Insured** to the **Underwriting Manager** or **Underwriter** and those publicly available in connection with the underwriting of this Policy.
- B. Attorney in Fact** means :
Mr. Sean Murphy
Attorney in Fact in Canada
for Lloyd's Underwriters
1155 rue Metcalfe, Suite 2220
Montreal, Quebec H3B 2V6
Canada
- C. Claim** means:
- (i) a written demand for monetary or non-monetary damages,
 - (ii) a civil proceeding commenced by the service of a complaint or similar pleading,
 - (iii) a criminal proceeding commenced by the return of an information or indictment,
 - (iv) a formal administrative or regulatory investigation, or proceeding commenced by the receipt by the **Insured** of a complaint made to the Privacy Commissioner, or similar regulatory or governmental official, or
 - (v) with respect only to Insuring Clause B, a written report by the **Insured** to the **Underwriter** of an actual or potential **Privacy Breach**.
- D. Claim Expenses** means reasonable costs, charges, fees (including but not limited to solicitors' fees and experts' fees) and expenses (other than regular or overtime wages, salaries or fees of directors, officers or employees of the **Insured Organization** or any **Subsidiary**) incurred in defending or investigating **Claims**, or circumstances which might reasonably lead to a **Claim** if incurred by the **Underwriter** or by the **Insured** with the prior written consent of the **Underwriter**, and the premium for appeal, attachment or similar bonds.
- E. Computer System** means computer hardware, software, and the data stored thereon, together with

associated input and output devices, networking equipment and electronic backup facilities.

- F. Crisis Management Expenses** means those reasonable and necessary expenses incurred by the **Insured** and approved by the **Underwriter** in retaining the services of a public relations firm and for related advertising or communication expenses at the direction of the said firm, solely for the purpose of averting or mitigating any material damage to the **Insured's** brand or reputation as a result of an actual or potential **Wrongful Act**.
- G. Denial of Service Attack** means an event that is caused by a third party's malicious activity which restricts or prevents access to an **Internet** or **Intranet** site or **Computer System** of another third party authorized to access same.
- H. Downstream Attack** means:
- (i) The **Unauthorized Use** of or **Unauthorized Access** to the **Computer System** of a third party provided such is attained through the **Insured's Computer System**;
 - (ii) The participation by the **Insured's Computer System** in a **Denial of Service Attack** directed against the **Computer System** of a third party; or
 - (iii) The transmission of **Malicious Code** from the **Insured's Computer System** to the **Computer System** of a third party.
- I. Extended Reporting Period** means the period of time after the end of the **Policy Period** for reporting **Claims** as provided in Section 9 of this Policy.
- J. Insured Person** means :
- (i) any past, present or future director, officer, trustee, employee, including temporary, part-time or leased employees, general or managing partner, or principal of the **Insured Organization** or a **Subsidiary**, but only while acting on behalf of or in the interest of the **Insured Organization** or a **Subsidiary**
 - (ii) independent contractors of the **Insured Organization** or of a **Subsidiary** who are natural persons, but only with respect to **Wrongful Acts** within the scope of such person's duties performed on behalf of the **Insured Organization** or of a **Subsidiary**.
- K. Insured**, either in singular or plural, means
- (i) the **Insured Organization**;
 - (ii) **Subsidiaries** of the **Insured Organization**, and
 - (iii) **Insured Persons**
- L. Insured Organization** means those organizations designated in Item 1 of the Declarations.
- M. Intranet** mean a private computer network inside a company or organization that uses the same kinds of software found on the **Internet**, but only for internal use.
- N. Internet** means the worldwide public network of computer networks which enables the transmission of electronic data between different users, including a private communications network existing within a shared or public network platform.
- O. Interrelated Wrongful Acts** means all causally connected **Wrongful Acts**.
- P. Loss** means the total amount the **Insured** is legally obligated to pay on account of each **Claim** and for all **Claims** in each **Policy Period** and the **Extended Reporting Period**, if exercised, made against it for **Wrongful Acts** for which coverage applies, including but not limited to, damages, judgments, settlements, costs, prejudgment or post-judgment interest, **Claim Expenses**, **Notification Expenses**

and **Crisis Management Expenses**, and fines, punitive and exemplary damages to the extent such are insurable under the most favorable laws of any jurisdiction which has a substantial relationship to the **Insured**, the **Underwriter**, this Policy or such **Claim. Loss** does not include:

- (i) future profits, restitution, or disgorgement of profits by any **Insured**
- (ii) the cost to comply with orders granting injunctive or non-monetary relief, including specific performance, or any agreement to provide such relief
- (iii) return or offset of fees, charges, royalties or commissions for goods or services already provided or contracted to be provided
- (iv) penalties of any nature, however denominated, arising by contract; and
- (v) matters uninsurable under the law pursuant to which this Policy may be construed.

- Q. Malicious Code** means unauthorized and corrupting or harmful computer code, including but not limited to computer viruses, spyware, Trojan horses, worms, logic bombs, and mutations of any of the proceeding.
- R. Network Security** means those acts, errors or omissions of the **Insured**, or others on behalf of the **Insured**, to protect against **Unauthorized Access to, Unauthorized Use of, Theft of Data from, Denial of Service Attack** directed against or transmission of **Malicious Code** to the **Insured's Computer System**.
- S. Notification Expenses** means those reasonable and necessary expenses incurred by the **Insured** and approved by the **Underwriter** solely to comply with governmental privacy legislation or guidelines mandating, or recommending as best practice, notification in the event of a **Privacy Breach**, including but not limited to reasonable communication expenses through, mail, call center and web site, and credit monitoring.
- T. Pending and Prior Litigation date** means the date specified in Item 6 of the Declarations.
- U. Policy aggregate limits** means the aggregate limit for this Policy set forth in Item 3A of the Declarations.
- V. Policy period** means the period of time from the effective date to the expiration date specified in Item 2 of the Declarations, or any earlier cancellation date.
- W. Privacy Breach** means a statutory, regulatory or common law breach of confidence, infringement, or violation of any rights to privacy, resulting in harm to employees of the **Insured** or third parties, including but not limited to unauthorized access to or collection, use, or disclosure of a person's personal information, breach of the **Insured's** privacy statement, breach of a person's right of publicity, false light, intrusion upon a person's seclusion, or misappropriation of a person's picture or name for commercial gain.
- X. Retroactive Date** means the date specified in Item 5 of the Declarations.
- Y. Subsidiary(ies)** means any organization, including but not limited to any corporation, partnership, limited liability corporation, unlimited liability corporation, association, trust or other entity in which the **Insured Organization** either directly or indirectly:
- (i) holds or controls the majority of the voting rights;
 - (ii) has the right to appoint or remove or otherwise controls a majority of the board of directors, or board of trustees, or functional equivalent; or
 - (iii) holds more than half of the issued equity capital.
- Z. Theft of data** means the unauthorized taking, misuse or disclosure of information on **Computer Systems**, including but not limited to charge, debit, and credit information, banking, financial and investment services account information, proprietary information, and personal, private and confidential

information.

- AA. Unauthorized access** means the gaining of access to a **Computer System** by an unauthorized person or persons or an authorized person in an unauthorized manner.
- BB. Unauthorized use** means the use of a **Computer System** by an unauthorized person or persons or an authorized person in an unauthorized manner.
- CC. Underwriter** means the insurance companies and underwriters at Lloyds of London, England, whose names appear below. The following underwriters have duly authorized Executive Risk Insurance Services Ltd, as the **Underwriting Manager**, to execute and sign this Policy on their behalf under Contract No N34327 in the following proportion:

Brit Syndicates Ltd 100%
Syndicate 2987 at Lloyd's

- DD. Underwriter Manager** means:

Executive Risk Insurance Services Ltd
365 Bay Street, 12th floor
Toronto, Ontario M5H 2V1
Canada

- EE. Wrongful Act** means any error, misstatement, misleading statement, act, omission, neglect, or breach of duty committed, attempted or allegedly committed or attempted by an **Insured**, with respect to its duties as such, resulting in:
- (i) With respect only to Insuring Agreement A and B, an actual or potential **Privacy Breach**; or
 - (ii) With respect only to Insuring Agreement C, a failure of **Network Security**, including such failure that results in a **Downstream Attack**.



NOTICE TO ASSUREDS Pursuant to the Freedom Of Information And Protection of Privacy Act, 1987

IMPORTANT

The notices below applies to insurance contracts containing non-automobile legal liability coverages in provinces where statistical data relating to such contracts must be reported to the Superintendent of Insurance and Lloyds Canada.

LEGAL AUTHORITY FOR COLLECTION

Insurance Act, R.S.O. 1990, c.I.8, section 101(1).

PRINCIPAL PURPOSE FOR WHICH PERSONAL INFORMATION IS INTENDED TO BE USED

Information collected by Underwriters from Assureds or supplied to Assureds pertaining to the attached document will be used:

- to compile aggregate statistical data to be used in monitoring trends in the insurance industry;
- to develop statistical exhibits to be used in monitoring the insurance industry;
- to respond to requests for customized statistical information on the insurance industry;
- to respond to inquiries on statistical information made to Office of the Superintendent of Insurance; and
- to use and disclose such information for purposes which are consistent with the previous clauses.

THE PUBLIC OFFICIAL WHO CAN ANSWER QUESTIONS ABOUT THE COLLECTION IS:

Manager, Statistical Services
Financial Services Commission of Ontario
5160 Yonge Street, 17th Floor
Box 85
North York, Ontario
M2N 6L9

Telephone (416) 250-7250
Fax (416) 590-7070

Notice concerning Personal Information

By purchasing insurance from certain Underwriters at Lloyd's, London ("Lloyd's"), a customer provides Lloyd's with his or her consent to the collection, use and disclosure of personal information, including that previously collected, for the following purposes:

- the communication with Lloyd's policyholders
- the underwriting of policies
- the evaluation of claims
- the detection and prevention of fraud
- the analysis of business results
- purposes required or authorized by law

For the purposes identified, personal information may be disclosed to Lloyd's related or affiliated organizations or companies, their agents/mandataries, and to certain non-related or unaffiliated organizations or companies.

Further information about Lloyd's personal information protection policy may be obtained from the customer's broker or by contacting Lloyd's on 514-861-8361 or through info@lloyds.ca.

Executive Risk Services 365 Bay Street, 12th Floor, Toronto, Ontario, Canada M5H 2V1, T: 416 979 3600, F: 416 979 8337

SCHEDULE C

Sample Privacy Policy Application



Executive Risk Insurance Services Limited

PRIVACY AND NETWORK LIABILITY INSURANCE APPLICATION

NOTICE: THIS IS AN APPLICATION FOR A CLAIMS MADE POLICY. THE POLICY ALSO PROVIDES THAT THE LIMITS OF LIABILITY AVAILABLE TO PAY JUDGEMENTS OR SETTLEMENTS SHALL BE REDUCED BY AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES. FURTHER NOTE THAT AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES SHALL BE APPLIED AGAINST THE RETENTION AMOUNT.

In the application, "PIPEDA" refers to the Personal Information Protection and Electronic Document Act; "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, and any amendments thereto; "G-L-B" refers to Gramm-Leach-Bliley Act and any amendments thereto.

In the event more space is needed to fully answer a question, please attach separate sheet(s) to this Application with the full answer.

Please attach copies of:

1. Privacy Policy and/or Statement currently in use
2. Most recent CA Letter to Management and Management's Response
3. Most recent network security and/or privacy audit

I. GENERAL INFORMATION

1. Name of Applicant:

Address of Applicant (Head Office Location):

Corporate Website:

2. Applicant Type

Individual: Corporation: Partnership: Other:

3. Date of Incorporation/Formation:

4. Jurisdiction of Incorporation/Formation:

5. Nature of Business:



6. Please list all direct and indirect Subsidiaries. (If included as an attachment, check here:)
 (If none, check here: "none".)

Name	Business or Type of Operation	Percentage of Ownership	Date Acquired or Created	Country of Incorporation

7. Proposed Effective Date:

8. Requested Retroactive Date (Policy Inception Unless Otherwise Stated):

9. Limit of Liability Desired:
- \$1,000,000
 - \$2,000,000
 - \$3,000,000
 - \$5,000,000
 - \$10,000,000

Other:

10. Retention Options Desired:
- \$25,000
 - \$50,000
 - \$100,000
 - \$250,000
 - \$500,000

Other:

II. EXPOSURE INFORMATION

Annual Revenue and Exposure Base

Past Accounting Year Total Revenues:
 Project Current Year Total Revenues:
 Estimate of Total Number of Individual Customer or Individual Patients:
 (Note: Patients if a Healthcare Applicant)

Employee and Independent Contractor Information

Total Number of Employees:
 Total Number of Employees, including directors and partners, who have access to sensitive employee or third party information:
 Total Number of Independent Contractors providing business process outsourcing or IT outsourcing to the Applicant:

11. Any significant changes in nature or size (more than 5% of revenues) of Applicant's business anticipated over the next twelve months? Yes No

If "Yes", please explain:



12. Provide the name of the Chief Security Officer (CSO), the Chief Privacy Officer (CPO) or the name/title of the individual(s) responsible for privacy/security regulatory compliance.

Name(s) / Title(s):

What proportion of their time is spent on privacy and/or security regulatory compliance?

13. Can the CPO or CSO confirm that they have reviewed the requirements of PIPEDA or any other applicable privacy legislation? Yes No

III. COMPLIANCE QUESTIONS

Please provide specific clarifications or exceptions to the following questions in the space provided or by attachment to this application. If any question does not apply to the Applicant, enter N/A (not applicable).

Healthcare Related Applicants Only

14. Is the Applicant and/or its subsidiaries a custodian or trustee of personal health information? Yes No

15. Does the Applicant and/or its subsidiaries process personal health information on behalf of third parties? Yes No

16. Is the Applicant and/or its subsidiaries subject to health privacy protection laws such as Ontario's Personal Health Information Protection Act, or similar legislation in other provinces? Yes No

If "Yes", please specify which province(s): _____

17. Does HIPAA apply to the Applicant and/or its subsidiaries? Yes No

If "Yes", do any of the following categories apply to the Applicant and/or its subsidiaries?

- a) Employees covered under a company self insured medical plan Yes No
- b) Health Care Provider Yes No
- c) Health Care Plan or Clearinghouse or Covered Entity Yes No
- d) Business Associate Yes No

Financial Services Applicants Only

18. Is the Applicant and/or its subsidiaries a federally regulated financial institution? Yes No

19. Is the Applicant and/or its subsidiaries a provincially regulated financial institution? Yes No

20. Does G-L-B apply to the Applicant and/or its subsidiaries as a bank or financial institution? Yes No

All Applicants

21. Does PIPEDA apply to the Applicant and/or its subsidiaries with respect to customer personal information? Yes No



22. Does PIPEDA apply to the Applicant and/or its subsidiaries with respect to employee personal information? Yes No
23. Do any provincial privacy statutes (such as the Personal Information Protection Act of B.C. or Alberta or the Quebec Act) respecting the protection of personal information in the private sector apply to the Applicant and/or its subsidiaries with respect to customer and/or employee personal information? Yes No

If "Yes", please identify the applicable province(s): _____

24. Has the Applicant and/or its subsidiaries conducted privacy/security compliance audits in the last 12 months?
- a) Privacy Impact Assessment for compliance with PIPEDA or any substantially similar provincial legislation? Yes No
 - b) Internal audit to determine compliance with regulations and laws concerning the protection of privacy rights? Yes No
 - c) Network Security Policies and Procedures Audit? Yes No
 - d) Audit and Certification from a Qualified Security Assessor (as that term is defined by the PCI Security Standards Council) as to compliance with the PCI-DSS? Yes No
 - e) Network Penetration Test? Yes No
 - f) HIPAA Privacy Audit (if applicable)? Yes No
 - g) HIPAA Security Audit (if applicable)? Yes No
 - h) G-L-B Audit (if applicable)? Yes No

If "Yes", please attach copies where applicable.

If 'Yes' to any of the above, who conducted the compliance audit? Scope of audit (all specific entities?)

Date completed:

- Did the compliance audit include a risk assessment or gap analysis? Yes No
- Did the compliance audit review written policies and procedures? Yes No
- Did the compliance audit review address privacy/security regulations? Yes No
- Did the compliance audit confirm that training programs are in place for ongoing guidance of employees regarding privacy/security regulations? Yes No
- Did the compliance audit confirm that IT security plan is periodically tested and updated to keep pace with changing technology and threats? Yes No
- Were all the audit recommendations requiring remediation by the Applicant accomplished? Yes No
- Was the remediation confirmed or retested by the auditor? Yes No
25. Does the Applicant and/or its subsidiaries collect payment card data? Yes No
26. Is the Applicant and/or its subsidiaries subject to PCI-DSS? Yes No
- If "Yes" what level requirement 1 2 3 4
- a) Has the applicant achieved PCI Compliance? Yes No
- If "Yes" please attach Certificate of Compliance
- If "No" please describe current status and timetable for compliance:



- critical and sensitive computer systems? Yes No
38. Does the Applicant have physical security controls in place to control access to computer systems? Yes No
39. Does the Applicant have an information security incident response plan in place including a System Event Log review process? Yes No
40. What are the estimated number of hours it would take to restore the Applicant's operations after a computer attack or other loss/corruption of data? _____
41. Does the Applicant use Encryption technology (specify what level) for protected personal information? Yes No
42. Does the Applicant use Encryption technology (specify what level) for all data stored on mobile devices (e.g. laptops)? Yes No
43. Does the Applicant have a person or group responsible for information security? Yes No
44. Does the Applicant use standard configurations for firewalls, routers and operating systems? Yes No
45. Do any of the above responses represent services performed by external service providers? Yes No
If "Yes", please specify:

V. HISTORICAL INFORMATION

46. Within the past three years, has the applicant experienced a security breach? Yes No
If "Yes", please provide the following information:
a) Cause:
b) Date of occurrence:
c) Damage or loss suffered:
d) Actions taken to prevent its reoccurrence:
47. Within the past three years, has the applicant experienced a privacy complaint or investigation? Yes No
If "Yes", please provide the following information:
e) Cause:
f) Date of complaint/investigation:
g) Results of investigation:
h) Actions taken to prevent its reoccurrence:
48. During the past three years, has the Applicant experienced an interruption or suspension of its computer system for any reason, which exceeded 4 hours and affected third party users/customers (not including downtime for planned maintenance)? Yes No
If "Yes", please provide the following information indicating:
a) the date and duration of the interruption or suspension:
b) the cause of the interruption:
c) amount of third party damages, loss, litigation arising out of the interruption or suspension:
49. Has any insurance policy providing the same or similar insurance as the insurance sought by this application ever been declined, non-renewed or cancelled during the past five years? Yes No
If "Yes", please provide the reason:



50. Has the Applicant suffered any loss or has any claim whether successful or not ever been made against the Applicant that would be covered by this insurance (includes all pending or prior claims, demand, suit, arbitration, litigation, bankruptcy, administrative proceeding or regulatory proceeding)? Yes No

If "Yes", please provide the following information with respect to each prior or pending matter indicating:

- a) the date that the prior or pending matter was first made:
- b) the date the Applicant first became aware of the matter:
- c) the names(s) of the party(ies) involved:
- d) a short description of the prior or pending matter and its current status:

51. Does the Applicant have knowledge or information concerning any act, error, omission, fact, circumstance, matter, incident or occurrence that could reasonably be expected to give rise to a claim or loss under the insurance sought? Yes No

If "Yes", please provide the following information with respect to each matter:

- a) description of circumstances:
- b) the date the matter first occurred:
- c) the date the Applicant first discovered it:
- d) any actions taken by the Applicant with respect to the matter:

52. Has any partner or director of the Applicant or its subsidiaries been found guilty of any criminal, dishonest or fraudulent activity or been investigated by any regulatory body? Yes No

If "Yes", please provide details:

It is agreed that with respect to Questions 49, 50 and 51 above, if such knowledge, information or involvement exists, any claim or action arising there from is excluded from the proposed coverage.



The undersigned persons declare that to the best of their knowledge the statements set forth herein are true and correct and that reasonable efforts have been made to obtain sufficient information from each and every Director or Officer or Trustee proposed for this insurance to facilitate the proper and accurate completion of this APPLICATION. The undersigned further agrees that, if between the date of this APPLICATION and the effective date of this Policy, (1) any material change in the condition of the Applicant is discovered, or (2) there is any material change in the answers to the questions contained herein, either of which would render this APPLICATION inaccurate or incomplete, notice of such change will be reported to the Underwriting Manager immediately and if necessary any outstanding quotation may be modified or withdrawn.

The signing of this APPLICATION does not bind the undersigned to purchase this insurance, but it is agreed by the Applicant and all persons proposed for this insurance that the particulars and statements contained in this APPLICATION and attachments and materials submitted with this APPLICATION (which shall be retained on file by the Underwriting Manager and shall be deemed attached to the Policy, if insurance is provided, as if physically attached thereto) are true and correct and will be the basis of the Policy and will be considered as incorporated in and constituting part of this Policy. It is further agreed by the Applicant and all persons proposed for this insurance that such particulars and statements are material to the decision to provide this insurance and that any Policy will be issued in reliance upon the truth of such particulars and statements. All such particulars and statements shall be construed as a separate APPLICATION for coverage by each person and no statement or omission in this APPLICATION or materials submitted with it, or knowledge possessed by any person shall be imputed to any other person for the purpose of determining if coverage is available. Statements or omissions in this APPLICATION or the attachments and materials submitted with it, or knowledge possessed by any of the Chief Executive Officer, Chief Financial Officer, Chief Privacy Officer, Chief Technology Officer (or any equivalent position) and any Director shall be imputed to the **Insured Organization** and any **Subsidiaries** for the purpose of determining coverage under the Policy.

PLEASE NOTE: ONLY DULY APPOINTED LICENSED BROKERS ARE AUTHORIZED TO SOLICIT APPLICATIONS FOR COVERAGE. BROKERS ARE NOT AUTHORIZED TO BIND COVERAGE. NO COVERAGE SHALL BE PROVIDED UNLESS THE UNDERWRITING MANAGER ACCEPTS THE APPLICATION AND BINDS THE COVERAGE. TAXES DUE UPON THE INCEPTION DATE OF THE POLICY ARE THE RESPONSIBILITY OF THE APPLICANT.

False information:

Any person who, knowingly and with intent to defraud any insurance company or other person, files an Application for insurance containing any false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act which is a crime.

This clause applies to the Province of Quebec only

It is the express wish of all parties that this application and any related documents be drawn up and executed in English. Les parties conviennent que la presente proposition et tous les documents s'y rattachant soient rédigés et signés en anglais.

Signature of Risk Manager

Signature of Chief Privacy Officer or Chief
Financial Officer

Date:

Date: