¶43-700 PRIVACY LIABILITY AND INSURANCE

Prepared by Murn Meyrick, CEO
Grey Swan Advisory Professional Corporation

¶43-701 OVERVIEW

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, or 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.

¶43-701a Roadmap: Navigating this Chapter

Quick Solutions:

- Use checklists and charts:
  - Map: Canadian Privacy Laws (¶43-742)
  - Checklist: Reviewing and developing a privacy liability risk management program (¶43-744a)
  - Checklist: Responding to a privacy breach (¶43-744b)
- Check key current trends and topics relating to privacy liability and insurance (¶43-701d):
  - New tort of invasion of privacy
  - Greater opportunity to bring claims without proving harm
  - Call for stronger enforcement measures
  - Cloud-based computing
  - Quebec's rise in privacy breach class actions
  - Increasing significance and purchase of privacy insurance
  - Contractual obligations for privacy liability insurance on the rise

Essential Preliminary Information and Organizational Context:

- Context for privacy liability and insurance (¶43-701b):
  - Data collection; privacy risks; privacy legislation and consequences of breach (Canadian and US developments); risk management solutions; global examples of privacy breaches and consequences; recent examples of Canadian privacy breaches
- Privacy legislation and its effects (¶43-701c):
  - Common themes; privacy regulation in Canada; key tenets under PIPEDA; breach notification requirements under privacy legislation in Canada; legislative responses to identity theft; other requirements addressing privacy concerns

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 1

Manage Legal Risk and Provide Advice:

- Role of in-house counsel in relation to privacy liability and insurance (¶43-704):
  - Advising the board of directors; participating in the privacy liability risk management solution; reviewing privacy liability insurance policies/coverage; reviewing/advising on contractual privacy liability insurance obligations
- Determining privacy risk exposures (¶43-706):
  - Sector; number of employees/customers; smaller companies lacking robust preventative programs; high-profile companies; sharing information with third parties; international aspects
- Identifying losses associated with a privacy breach (¶43-708):
  - Third-party liability; regulatory/law enforcement costs; first party/direct damages to business
- Best practices to reduce and manage privacy breach risks:
  - Privacy Commissioner guidance; recommended best practices: provide leadership; educate employees; encrypt data; develop retention and destruction policy; implement preventive measures; develop incident response plan (¶43-710a)
  - Additional risk mitigation measures: risk identification and adoption of security measures; contractual indemnities; insurance coverage
- Managing privacy risks through insurance:
  - Privacy liability insurance terminology (¶43-712a)
  - Integrating privacy liability insurance into a risk management program (¶43-712b)
  - Understanding limitations on coverage under traditional insurance policies (¶43-712c)
  - Highlights of privacy and network security insurance (¶43-712d)
  - Limits of liability and insurance market capacity (¶43-712e)
  - Purchasing coverage for privacy risks (¶43-712f)

Conduct Further Research:

- Link to key cases involving privacy breaches (¶43-772)
- Link to key privacy legislation by jurisdiction (¶43-774)
- Link to privacy commissioners by jurisdiction (¶43-792)

¶43-701b The Context for Privacy Liability and Insurance

- ***Data collection:*** Governments and businesses collect and store sensitive private information relating to their customers and employees on a scale and in formats previously unimaginable (e.g., cloud-based computing and powerful data mining software). Social networking websites (such as Facebook, Google+, Twitter, and LinkedIn) have become the established norm for communicating and maintaining relationships. Vast data collections can be accessed and processed virtually instantaneously from around the world. New and emerging technologies — including facial recognition software, wearable computing, smart phones, and drones — raise privacy challenges. Unauthorized access to or disclosure of data (both in electronic and hard copy) has given rise to significant exposure. These risks arise not only from sophisticated hackers, but also from simple negligence, such as lost laptops or mobile devices.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 2

© 2015, CCH Canadian Limited

- ***Privacy and cyber risks:*** The privacy risks associated with technological advances in accessing personal information are substantial:
  - ***Cyberattacks:*** Vast amounts of sensitive, private information and sensitive business information stored in accessible formats can fall into criminal hands by sophisticated hackers breaching network security, or by simple negligence. The escalating cyberattacks are not limited to data breaches — they also include extensive network attacks and threats to destroy or corrupt data.
  - ***Security breaches:*** Installation of viruses or malware can damage a company's systems and lead to the theft of more data. Criminals may extort companies desperate to restore computer networks. Business may be interrupted through disabled or corrupt databases. On a less sinister basis, the problem of web leakage, in which the personal information of a site's registered users seeps through to third parties such as advertisers, is a growing problem.
  - ***Investigations and litigation:*** Regulatory and criminal investigations, class action litigation, and individual lawsuits relating to privacy breaches are no longer just hypothetical, they are a new reality. The actions tend to involve disclosure of personal information through insecure disposal of records, theft and loss of unencrypted data on mobile devices, and unauthorized access to or use of records. Despite significant costs associated with defending regulatory or legal actions, one of the largest exposures for a company experiencing a privacy breach is the reputational damage.
  - ***Director and officer exposure:*** The high severity cyberbreaches of 2013 and 2014 brought with them significant director and officer exposure, both in terms of regulatory investigation and enforcement, as well as derivative lawsuits. Questions are being asked about whether companies adequately guarded data, had in place sufficient internal controls, and informed investors about the impact of breaches. In a June 10, 2014 speech, Securities Exchange Commissioner Luis Aguilar said "ensuring the adequacy of a company's cybersecurity measures needs to be a part of a board of director's risk oversight responsibilities" and that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."[1]
- ***Privacy legislation and consequences of breach:*** Legislative and regulatory initiatives around the globe in past years have made data privacy and security issues a top corporate priority as the potential losses are enormous and constitute a key business threat.
  - ***Canadian developments:*** The reality in Canada is that the regulatory environment has not kept pace with the escalating scope of the risk. As a step in the right direction, Canada's anti-spam law ("CASL") finally came into force on July 1, 2014.[2] CASL is an onerous regime with serious ramifications, including significant penalties (up to $1 million for individuals and $10 million for others), director and officer liability, and damages. On the other hand, unlike many jurisdictions around the globe, Canada has failed to pass comprehensive laws mandating a response to a breach. With breaches and losses mounting, Canadian regulators are clamouring for legislative clout to impose significant consequences where breaches do occur.[3]
  - ***US developments:*** In October 2011, the US Securities and Exchange Commission issued disclosure recommendations making it best practice to disclose material information regarding cybersecurity risks and incidents.
- ***Risk management solutions:*** Corporations are closely examining risk management solutions to reduce their exposure, including assessment of new insurance solutions. Many companies are unlikely to be able to avoid risk altogether and even the best of security protections may not be enough to avoid all

[1] SEC Commissioner Aguilar Addresses Cybersecurity Oversight Responsibilities of Corporate Boards, The D&O Diary, June 12, 2014, available at http://www.dandodiary.com/2014/06/articles/cyber-liability/sec-commission-aguilar-addresses-cybersecurity-oversight-responsibilities-of-corporate-boards.

[2] Most of CASL and the regulations came into force July 1, 2014; however, additional sections are slated to come into force on January 15, 2015 (relating to installation of computer programs) and July 1, 2017 (private right of action and statutory damages).

[3] Privacy Commissioner of Canada, *Annual Report to Parliament 2012*, June 2013, available at https://www.priv.gc.ca/information/ar/201213/2012_pipeda_e.pdf.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\ucg\master\sf14201.dat Seq: 3

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.

- ***Global examples of privacy breaches and consequences:*** News headlines around the globe highlight the increasing frequency and severity of privacy breaches:

  – ***Home Depot Inc.:*** Malicious software installed mainly on payment systems at retail stores in both the United States and to a much lesser extent in Canada allowed hackers to steal an estimated 56 million credit and debit card numbers over a five-month period in 2014. The fallout has included class action suits launched in Canada, and estimates of costs into the billions.[4]

  – ***Target Corporation:*** Forty million customer credit and debit cards were exposed during a three-week period in December 2013 due to a malicious software program similar to that used in the Home Depot hacking. Stolen cards soon turned up for sale in an underground cybercrime shop. In the aftermath Target has reportedly spent $148 million, minus a $38 million insurance receivable, on data breach investigation, credit monitoring, call centre staff, legal fees, fraud losses, and card replacements.[5] Furthermore, Target's CEO stepped down in the midst of derivative lawsuits and regulatory investigations. The company experienced a 46 per cent drop in profits in Q4 compared to the year before; an estimated $200 million was given to credit unions and banks for reissuing compromised cards; an estimated $100 million is being spent by Target to upgrade their payment terminals; and one to three million of the stolen cards were successfully sold on the black market and used for fraud.[6]

  – ***Wyndham Worldwide Hotels:*** Wyndham experienced three data breaches during the period April 2008 to January 2010, allegedly resulting in the compromise of more than 619,000 consumer payment card account numbers, many of which were exported to a Russian domain, resulting in fraudulent charges and more than $10.6 million in fraud losses. A Federal Trade Commission enforcement action followed, as did a shareholder derivative action against certain directors and officers of Wyndham and the company itself.[7] Wyndham reportedly incurred significant expense in notifying affected individuals, providing credit card monitoring, and attempting to satisfy state regulators and attorneys general that it was adequately responding to the breaches.[8]

  – ***Winners/HomeSense:*** Another costly examples 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 US 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 US 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 faced litigation from stakeholders including consumers, banking associations, and shareholders. The settlement of the Canadian component of the class action by consumers resulted in eligible class members

[4] CBC News, "Home Depot admits 56 million cards hit by security breach", September 18, 2014, available at http://www.cbc.ca/news/business/home-depot-admits-56-million-cards-hit-by-security-breach-1.2770827.

[5] Forbes, "Target shares tumble as retailer reveals cost of data breach", August 5, 2014, available at http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/.

[6] Krebs on Security, "The Target breach, by the numbers", May 14, 2014, available at http://krebsonsecurity.com/tag/target-data-breach/.

[7] *Palkon, derivatively on behalf of Wyndham Worldwide Corporation v. Holmes et al.*, USDC Case 2:14-cv-01234-SRC-CLW filed 5/2/14.

[8] "Anatomy of a Hotel Data Breach", June 24, 2014, available at https://www.linkedin.com/pulse/article/20140-624024142-10004064-anatomy-of-a-hotel-data-breach.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 4

© 2015, CCH Canadian Limited

receiving credit monitoring services, vouchers, cash benefits, identity theft insurance, reimbursements and sales events. Total costs of the breach were said by TJX to be $171 million.

– ***Sony:*** In 2011, computer "hacktivists" unlawfully accessed the Sony PlayStation Network and obtained the financial and personal information of approximately 77 million video game users. Sony was criticized for not telling customers quickly enough about the breach.

Sony estimated the cost of remedying and mitigating the incident to be $171 million, including a fine in the United Kingdom of $390,000, responding to at least 58 lawsuits including class actions in Canada[9] and the United States, and a lawsuit by its commercial general liability insurer (Zurich American), which sought a declaration that its policies do not cover the losses arising from a data breach.[10]

In the wake of this massive breach, Canada's privacy commissioner publicly called for the power to impose "attention-getting fines" when major corporations fail to protect personal information.[11]

– ***Heartland Payment Systems Inc.:*** In January 2009, Heartland disclosed what is believed to be the largest ever data breach resulting from criminal hacking of an estimated 100 million credit and debit cards.

It was estimated that Heartland paid approximately $140 million in breach-related expenses, including $63.5 million to credit card companies, $42.8 million to fund proposed settlements with various litigants including consumer class actions, and more than $26 million in legal fees.

Although it appeared that settlements had been finalized in 2010, in 2013 a collection of banks involved in the settlements attempted to reopen their negligence case against Heartland. Heartland reportedly recovered tens of millions of their losses through insurance.[12]

– ***Facebook Apps:*** Facebook has had its share of privacy issues, including its highest profile problem in October 2012, when it admitted that its top 10 applications shared user data with advertisers. Tens of millions of users were affected.

The US Federal Trade Commission settled various issues with Facebook in November 2011, which included an agreement to 20 years of third-party privacy audits. Facebook was sued in Quebec and Manitoba, and a settlement was reached with the Canadian members of Facebook which called for an updated privacy policy to be maintained in the same form for at least three years, for payment of each plaintiff's counsel's fees up to $75,000, and a payment of $1,000 to the class representative.

In 2014, a class action in British Columbia was certified against Facebook alleging that Facebook used the names and likenesses of its customers for advertising without permission.[13] The Court dismissed Facebook's jurisdiction arguments that its Terms of Use precluded actions outside California and found that the BC *Privacy Act* applied. This decision is under appeal.[14]

• ***Recent examples of Canadian privacy breaches:*** Canada has similarly seen an explosion in breach incidents. In 2013, 69 per cent of Canadian companies reported having some kind of cyberattack over the past year.[15] About 25 per cent

[9] *The Toronto Star*, "PlayStation users plan class action suit for hacking", May 3, 2011, available at http://www.thestar.com/news/gta/2011/05/03/playstation_users_plan_class_action_suit_for_hacking.html.

[10] *Zurich American Insurance Co., et al. v. Sony Corp. of America, et al.*, No. 651982/2011 (NY Sup. Ct. NYC).

[11] *The Globe and Mail*, "Canada's privacy commissioner wants hefty fines for data breaches", May 4, 2011, available at http://www.theglobeandmail.com/technology/canadas-privacy-commissioner-wants-hefty-fines-for-data-breaches/article578748/.

[12] Christian Science Monitor, "Data theft: Top 5 most expensive data breaches", available at http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/4.-Heartland-Payment-Systems-140-million.

[13] *Douez v. Facebook, Inc.*, 2014 BCSC 953.

[14] "Canada: Two Privacy Class Actions: Facebook And Apple, Richard Stobbe", November 6, 2014, available at http://www.mondaq.com/canada/x/352316/Data+Protection+Privacy/Two+Privacy+Class+Actions+Facebook+and+Apple.

[15] International Cyber Security Protection Alliance report, available at https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 5

of those interviewed said that the attacks had a considerable impact on their business, both in terms of financial loss and reputational damage, with a total reported loss of more than $5 million. Canadian breach incidents have included:

– ***Bank of Nova Scotia:*** The case of *Evans v. The Bank of Nova Scotia*[16] is notable as being the first in Canada to be certified as a class action based on the tort of intrusion upon seclusion. The claim alleges that the bank should be held vicariously liable for an employee's deliberate breach of customers' privacy rights. The employee accessed personal information of 643 customers and provided such information to his girlfriend, who passed it along to third parties in an identity theft scam. Approximately 140 of those customers were victims of identity theft and/or fraud. The bank compensated affected customers who suffered losses (including fraudulently obtained credit cards, unauthorized purchases, account takeovers, etc.), and offered credit monitoring and identity theft protection services.

– ***Canada Student Loans Program:*** In early 2013, Human Resources and Skills Development Canada ("HRSDC") admitted to the loss of a portable hard drive containing unencrypted personal and financial information, including social insurance numbers and birth dates, pertaining to more than half a million people who took out student loans, as well as 250 employees. Reports allege that there had been a two-month delay in notifying the public of the breach.

  Within days, three class actions were launched and both the Royal Canadian Mounted Police and the Privacy Commissioner commenced investigations. Affected persons were notified by letter and a hotline was set up to handle inquiries (the hotline reportedly received over 40,000 calls). This announcement was followed by the disclosure by HRSDC of another breach involving the loss of a USB drive from an office in Quebec, containing the personal information of more than 5,000 Canadians.[17] On March 17, 2014, the Federal Court certified a class action that alleges that the federal government should be held liable for the tort of intrusion upon seclusion in failing to protect personal information.[18] The Court found that the frustration and anxiety experienced by violated individuals could potentially meet the threshold of "distress" set out by the Court of Appeal in *Jones v. Tsige*[19] as a requirement for a privacy breach claim. However, the Court found no evidence the affected individuals were at an increased risk of identity theft and thus their claim for compensable damages was dismissed, leaving them to pursue nominal damages only.

– ***Investment Industry Regulatory Organization of Canada ("IIROC"):*** In April 2013, an IIROC employee lost an unencrypted laptop containing the financial information of over 52,000 brokerage firm clients.

  The fallout included wide media reporting of the breach both in Quebec, and nationally, followed by the launch of a class action and multiple investigations, including one by the Canadian Securities Administrators. The breach reportedly cost IIROC about $5.7 million.[20] The class action was not authorized by the Quebec court (which decision is under appeal), in part because of the lack of harm to affected individuals (there were no known cases of identity theft or fraud resulting from the breach, and credit monitoring was offered by IIROC).[21]

– ***Elections Ontario:*** In early July 2012, Elections Ontario lost memory sticks containing the personal information of 2.4 million voters. Within a

[16] 2014 ONSC 2135.

[17] "Federal government faces third class-action lawsuit over privacy breach", January 13, 2013, available at http://www.ctvnews.ca/canada/federal-government-faces-third-class-action-lawsuit-over-privacy-breach-1.1120336.

[18] *Condon v. Canada*, 2014 FC 250.

[19] 2012 ONCA 32.

[20] Brokerages react apathetically to new regulatory boss, GlobeAdvisor.com, September 9, 2014, https://secure.globeadvisor.com/servlet/ArticleNews/story/gam/20140909/RBSWERMAN.

[21] *Paul Sofio v. OCRCVM (IIROC)*, 2014 QCCS 406.1.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 6

© 2015, CCH Canadian Limited

few weeks, a province-wide class action lawsuit was filed.

– ***Apple:*** The Quebec Superior Court authorized a class action against Apple and Apple Canada on June 27, 2014. The action alleges that Apple violated users' rights to privacy by transmitting or allowing apps to transmit private data to advertisers. This action mirrors similar actions filed in the United States.[22] On the other side of the country in British Columbia, a class action alleging Apple breached customers' rights to privacy by recording and storing locational data in unencrypted form which is accessible to Apple was dismissed.[23]

– ***Montfort Hospital:*** A group of 25,000 patients whose personal information was lost on a USB drive in November 2012 launched a class action suit against this Ottawa hospital.

– ***Prime Healthcare Services Inc.:*** This Ontario hospital chain was fined $95,000 (which was appealed) by California state regulators for the unauthorized disclosure of medical information resulting from the sharing of a woman's files with journalists and the sending of an email about her treatment to nearly 800 hospital employees. The patient filed a civil suit over the breach.

  In June 2013, Prime Healthcare agreed to pay $275,000 to settle a US federal investigation into alleged violations of patient privacy.

– ***Durham Region Health:*** In 2011, the Ontario Superior Court granted certification of a class action against Durham Region Health when a nurse employed by the Durham Region Health Department allegedly lost a USB drive containing personal and confidential health information relating to flu vaccinations given to patients. The action followed an investigation and order by the Ontario Information and Privacy Commissioner citing numerous breaches of the privacy health legislation.

  In the action, the plaintiffs sought $40 million in damages, citing risk of identity theft as a factor. The certification order, which was largely made with the consent of the defendants, required the defendants to pay for the costs of notifying the class members (approximately 83,500 patients) and for the costs of operating the program whereby individuals can opt-out of the action if they choose. The action was settled shortly after certification, with the Region agreeing to pay up to $500,000 on account of the plaintiffs' costs, and individual payments to those affected individuals who can prove financial loss.[24]

– ***Jones v. Tsige:*** In 2012, the Ontario Court of Appeal recognized the new common law tort of intrusion upon seclusion in the landmark decision of *Jones v. Tsige*.[25] The Court awarded $10,000 in damages to a man whose former wife, a bank employee, had inappropriately accessed personal banking information relating to her ex-husband's new partner 174 times. The Court imposed a cap of $20,000 where there has been no pecuniary loss, and although the possibility exists for punitive or aggravated damages on top of this amount, such damages would only be awarded in exceptional cases.

  It is important to note that this is a common law cause of action, separate and apart from any remedy under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[26] or other similar privacy legislation. It remains to be seen whether entities subject to PIPEDA or similar legislation will be subject to duties and remedies under both this new common law action and the relevant statute.

[22] *Albilia c. Apple inc.*, 2013 QCCS 2805, http://citoyens.soquij.qc.ca/php/decision.php?liste=69879788&doc=66BD2DAA835609FA824DE5CD4181681839-D49FDD135551BF12BC2F83CDCE6001&page=1.

[23] "Canada: Two Privacy Class Actions: Facebook And Apple", Richard Stobbe, November 6, 2014, available at http://www.mondaq.com/canada/x/352316/Data+Protection+Privacy/Two+Privacy+Class+Actions+Facebook+and+Apple.

[24] "The Cost of Losing Stuff — The Durham Health Class Action Settlement", available at http://carswellprivacylaw.wordpress.com/2012/06/14/the-cost-of-losing-stuff-the-durham-health-class-action-settlement/.

[25] 2012 ONCA 32, http://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.html.

[26] SC 2000, c. 5.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 7

This new tort will be available to plaintiffs in class actions alleging privacy breaches, even where no harm has been proven.

– ***Landry v. Royal Bank of Canada:***[27] In 2011, the Federal Court ordered a Canadian bank to pay damages in respect of a breach of the federal privacy legislation by one of its employees. Contrary to the bank's policies, the employee had, in response to a subpoena, provided private bank information to a customer's ex-spouse who was involved in a contested divorce.

Despite arguments challenging the cause of the complainant's alleged "humiliation" being related to the privacy breach, the Court found that the breach warranted damages in the amount of $4,500, plus interest and costs.

¶43-701c Privacy Legislation and its Effects

- ***Common themes of global privacy legislation:*** Privacy legislation worldwide contains many common themes, particularly to:
  - Address the collection, storage, and use of "personal information"[28] by both government agencies and the private sector;
  - Outline appropriate technical and organizational measures to protect such data; and
  - Outline the rights of individuals and potential sanctions for breach.
- ***Regulation of privacy in Canada:*** 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 few 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, with countries around the world demanding enhanced protections. In Canada, privacy is governed at both the federal and provincial levels, and certain sectors have additional requirements:
  - ***Federally regulated workplaces — PIPEDA:*** The personal information in federally regulated workplaces (such as telecommunications, broadcasting, and local businesses in Yukon, Nunavut, and Northwest Territories) is protected under PIPEDA.[29]
  - ***Federally regulated public bodies — Privacy Act:*** The personal information of federally regulated public bodies (including Bank of Canada, Canada Revenue Agency, Canadian Space Agency, National Research Council of Canada, Statistics Canada, and Treasury Board of Canada) is governed by the federal *Privacy Act*.[30]
  - ***Private sector — Provincial and federal legislation:*** In the provinces of Alberta, British Columbia, Manitoba, and Quebec, privacy for private sector organizations is protected under statutes "substantially similar" to PIPEDA (see "Privacy Laws by Jurisdiction" at ¶43-774). All other provinces must comply with PIPEDA.
  - ***Health information:*** Ontario, New Brunswick, and Newfoundland and Labrador have their own specific privacy legislation which applies to health information (see "Privacy Laws by Jurisdiction" at ¶43-774).
  - ***Public sector:*** Each province and territory has its own public sector privacy legislation (see "Privacy Laws by Jurisdiction" at ¶43-774).
- ***Key tenets under PIPEDA:*** The following 10 privacy principles outline the responsibilities that organizations subject to PIPEDA must follow:
  1. ***Accountability:*** The organization must designate someone to be accountable for the management of personal information, usually called the Privacy Officer.
  2. ***Identifying purpose:*** The organization must clearly identify the purposes for which personal

[27] *Landry v. Royal Bank of Canada*, 2011 FC 687.

[28] "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.

[29] SC 2000, c. 5.

[30] RSC 1985, c. P-2.1.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 8

© 2015, CCH Canadian Limited

information is collected, either before or at the time of collection.

3. ***Consent:*** Knowledge and consent is required when an organization collects, uses, or discloses personal information and it must be in such a way that can be clearly understood.
4. ***Limiting collection:*** The personal information collected should be limited to that which is necessary for the identified purpose.
5. ***Limiting use, disclosure, and retention:*** The way an organization uses, discloses, and retains personal information must be limited to its received consent and identified purposes.
6. ***Accuracy:*** The organization must ensure that the personal information it collects is accurate, complete, and up-to-date for the purposes for which it is being used.
7. ***Safeguards:*** The organization should protect personal information with security safeguards that are appropriate for the sensitivity of the information held.
8. ***Openness:*** The policies and procedures about how personal information is managed should be readily available.
9. ***Individual access:*** Upon request, the existence, use, and disclosure of personal information must be made known to an individual, and access to it must be provided.
10. ***Challenging compliance:*** Individuals must be able to challenge an organization's compliance on any of the privacy principles of PIPEDA.

- ***Breach notification requirements under privacy legislation in Canada:***
  - ***Provincial — Alberta and Manitoba:*** Alberta requires mandatory breach notification for private sector companies.

    In May 2010, amendments to Alberta's *Personal Information Protection Act*[31] came into force, which include the requirement to notify the Alberta Information and Privacy Commissioner of a privacy breach that poses a real risk of significant harm to individuals. The Commissioner then decides whether individuals should be notified and if so, how.

    Further, the amendments institute a new offence for failure to comply with the notification requirement and for obstructing the Commissioner in his or her investigations of privacy breaches.

    In September 2013, Manitoba enacted new privacy legislation,[32] which has not yet been proclaimed into force. It contains a broadly worded breach notification obligation, requiring notice to affected inviduals if personal information is "stolen, lost or accessed in an unauthorized manner". An exception exists if the organization is "satisfied that it is not reasonably possible for the personal information to be used unlawfully".
  - ***Provincial health information:*** A number of provinces, including Alberta, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Quebec, Saskatchewan, and Yukon have breach notification requirements applicable to personal health information only. Please see the chart of privacy legislation across Canada at ¶43-774.
  - ***Federal:*** Legislation requiring mandatory breach notification applies to public sector organizations only. No such requirement is applicable to private sector companies, despite lengthy consideration.

    Parliament is currently considering Bill S-4 (the government's third attempt since 2010), which would amend PIPEDA,[33] to force organizations to notify the federal privacy commissioner and any affected individuals of a breach of personal information that poses a "real risk of significant harm" to an individual. Additionally, all breaches must be recorded and reported to the Commissioner upon request.

[31] *Personal Information Protection Amendment Act, 2009* (SA 2009, c. 50) and the *Personal Information Protection Act Amendment Regulation* (AR 51/2010).

[32] *Manitoba Personal Information Protection and Identity Theft Prevention Act*, CCSM c. P-33.7.

[33] Bill S-4, *Digital Privacy Act.*

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 9

Bill S-4 would improve the current situation where there is no disclosure requirement, and would be an improvement over prior Bills in that it: (1) provides more clarity (both a definition for "significant harm" and a non-exhaustive list of factors to consider in determining the existence of a "real risk"); (2) adds strength to the consequences for failure to comply (knowingly failing to report or record a breach would subject a company to fines of up to $100,000); and (3) adds a new power of the Commissioner to enter into a "compliance agreement" with a company that the Commissioner believes has committed, is about to commit, or is likely to commit a breach of PIPEDA. The Commissioner would have greater enforcement powers to compel compliance with such an agreement, including application to the Federal Court. 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.

- ***Legislative responses to 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. As of January 8, 2010 the Canadian *Criminal Code*[34] was amended, making 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.
- ***Other requirements addressing privacy concerns:*** 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. For example:
  - ***Payment Card Industry Data Security Standard ("PCI DSS"):***[35] PCI DSS is a global standard established to mandate robust security processes governing all merchants and organizations that store, process, or transmit payment card data, including prevention, detection, and appropriate reaction to security incidents.
  - ***Canadian Charter of Rights and Freedoms:***[36] Although the *Canadian Charter of Rights and Freedoms* does not specifically mention privacy or the protection of personal information, it does afford relevant protections under sections 7 (the right to life, liberty, and the security of the person) and 8 (the right to be secure against unreasonable search or seizure).
  - ***Collective agreements:*** Privacy in the workplace has become of sufficient concern that many trade unions are ensuring that protections are incorporated into collective agreements — for example, rights involving workplace surveillance and electronic monitoring.

¶43-701d Key Current Trends and Topics Relating to Privacy Liability Insurance

- ***New tort of intrusion upon seclusion:*** Ontario recognizes the new tort of intrusion upon seclusion (see discussion on *Jones v. Tsige* at ¶43-701b, above). Conversely, British Columbia does not. Specificially, in the recent judgment of the British Columbia Supreme Court in *Demcak v. Vo,*[37] the judge noted that there is no tort of invasion of privacy under the laws of that province, although a breach of privacy is actionable under BC's *Privacy Act*. Recently the issue of the availability of this common law tort in the context of health care has arisen. In *Hopkins v. Kay,*[38] the Ontario Superior Court held that the recourse available under Ontario's *Personal Health Information Protection Act*[39] ("PHIPA"), does not oust the common law

[34] RSC 1985, c. C-46.

[35] For more information, see https://www.pcisecuritystandards.org/security_standards/index.php.

[36] *Constitution Act*, 1982, c.11 (UK), Schedule B.

[37] 2013 BCSC 899, http://www.canlii.org/en/bc/bcsc/doc/2013/2013bcsc899/2013bcsc899.html.

[38] 2014 ONSC 321.

[39] SO 2004, c. 3.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 10

© 2015, CCH Canadian Limited

remedy. This case, which is currently under appeal, will be important as there exists considerable disparity in an individual's rights under PHIPA compared to the common law.[40]

- ***Greater opportunity to bring claims without proving harm:*** The Ontario Superior Court in *Jones v. Tsige* specifically noted that "proof of harm to a recognized economic interest is not an element of the cause of action" for the newly recognized tort of intrusion upon seclusion. Additionally, Canada's new anti-spam legislation[41] contains a private right of action without the requirement to prove harm.
- ***Call for stronger enforcement measures:*** As noted above, in the wake of significant privacy breaches in Canada including the Sony breach, there has been a regulatory cry for stronger enforcement measures in the event of serious breaches. In 2012, the federal Privacy Commissioner appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its study on social media and privacy calling for greater enforcement powers. Canada has been noted to be falling behind many other countries in its enforcement powers. It is predicted that enhanced enforcement will increase companies' exposures in terms of fines, penalties, responding to regulatory actions, and breach notification costs.
- ***Director and officer exposure:*** Cybersecurity represents a growing director and officer liability, as illustrated by the derivative lawsuits filed in the United States against Target[42] and Wyndham Worldwide, (see discussion on Target and Wyndham at ¶43-701b) following their high-profile breaches. In addition, such breaches have resulted in one or more of the Securities and Exchange Commission ("SEC"), Federal Trade Commission, and states' attorneys general investigations of management over the handling of cyberattacks, the strength of their internal controls, and whether the companies adequately guarded data and informed investors about the impact of the breaches. For financial firms, the pressure has heated up with the US Office of Compliance, Inspections and Examinations of the SEC (governing investment advisers and asset managers), and the Financial Industry Regulatory Authority becoming involved in a cyber crisis.[43]
- ***IP theft and impairment of company assets:*** Past cyber litigation dominated by consumer class actions will be joined by a growing exposure in the area of theft of intellectual property and impairment of company assets.
- ***Cloud-based computing:*** As more and more businesses recognize the power of cloud-based services and their ability to access and process limitless amounts of data at reduced capital costs and IT service expenses, there must be a corresponding recognition of the risks — data corruption and loss, unauthorized access, breach of law, and potential fines and penalties for directors and officers.
- ***Quebec's rise in privacy breach class actions:*** Robust privacy laws and the possibility of punitive damages increases a company's risks, as evidenced by a rise in privacy breach class actions in Quebec.[44]
- ***Increasing significance and purchase of privacy insurance:*** Many more insurers (reportedly 25–30) have entered the Canadian market and companies are no longer just talking about it but are actually buying it.
- ***Contractual obligations for privacy liability insurance on the rise:*** Contractual requirements for privacy liability insurance are becoming increasingly common in legal and financing agreements. Before entering into an outsourcing agreement where the third party will have access to a company's personal information, some parties are being required to show proof that they have privacy insurance in place as a backstop in case they should commit a privacy breach.

[40] The PHIPA framework precludes civil actions based on the common law until after the Privacy Commissioner has issued a conviction or a final order. Further, under PHIPA, damages are capped at $10,000 for mental anguish, whereas there is no cap under the common law, which also allows for aggravated and punitive damages.

[41] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c. 23.

[42] Kulla, derivatively on behalf of *Target Corporation v. Steinhafel, et al.* USDC Case 0:14-cv-00203-SRN-JSM filed 1/21/14.

[43] John Reed Stark, "Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught", April 21, 2014, http://www.strozfriedberg.com/wp-content/uploads/2014/04/Cybersecurity-and-Financial-Firms-Bracing-for-the-Regulatory-Onslaught_BloombergBNA_Stark_April2014.pdf.

[44] For example, *Alibilia c. Apple Inc.*, 2013 QCCS 2805; *LaRose c. Banque Nationale du Canada*, 2010 QCCS 5385.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 11

¶43-702 PRACTICAL APPLICATION

¶43-704 The Role of In-House Counsel in Relation to Privacy Liability and Insurance

The financial and reputational losses associated with privacy-related breaches underscore the importance for every organization of having a structured privacy program in place, properly training employees about their responsibilities relating to privacy, and ensuring that appropriate security processes are in place to respond to a breach and mitigate the risks.

- ***Advising the board of directors:*** Given the increasing risks associated with cybersecurity and related privacy issues, and the message regulators are spreading about the expectation of companies to take appropriate steps to guard against the risks and to be held accountable for their shortcomings, this topic is now reaching companies' boards of directors.

  In-house counsel must be prepared to answer directors' questions about what the company is doing to assess its exposures and to protect against them. In the United States, the Securities and Exchange Commission ("SEC") has provided guidance that specifically emphasizes that companies should be disclosing a "description of relevant insurance coverage" relating to cyber exposures.[45] To date no such requirement exists in Canada. In-house counsel must be prepared to answer the board's questions with respect to an assessment of steps taken to put insurance in place to protect against the risks.

- ***Participating in the privacy liability risk management solution:*** Depending on the size of the company, in-house counsel may be required to work with the following other internal positions in determining an appropriate privacy liability risk management solution: Risk Manager, Chief Financial Officer, Chief Privacy Officer, and Chief Information Officer. Insurance must be placed by a licensed insurance broker.

- ***Reviewing privacy and director and officer liability insurance policies/coverage:*** Given that these insurance policies are significant commercial contracts with complex non-standardized terms, legal review including expertise in privacy coverage is highly recommended. In-house counsel may wish to consult with external legal counsel or other consultants specialized in insurance law.

- ***Reviewing/advising on contractual privacy liability insurance obligations:*** It is common to see insurance requirements in standard service contracts; however, as an understanding of the limitations that traditional insurance provides to a privacy breach evolves, an emerging trend has been the development of a requirement for specific privacy liability insurance to be part of contractual obligations.

  In-house counsel should be aware of this and consider whether such a term should be included in the company's contractual provisions with its outsourced service providers and then conduct audits of the particulars of the insurance maintained by those service providers.

¶43-706 Determining Privacy Risk Exposures

A recent study of Canadian companies found that more than one-third knew that they had had a significant breach over the previous 12 months.[46] The same study found that the number of breaches could be higher since 56 per cent of the 236 Canadian respondents said they believed threats fall through the cracks of their security systems. Law firms, accounting firms, and similar professional companies have been said to be particularly at risk for privacy breaches due to the large number of sensitive records they hold and their lack of higher level security solutions available to larger financial institutions such as banks.

[45] Division of Corporation Finance, Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2 — Cybersecurity", October 13, 2011, available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[46] "Cyber attacks have hit 36 per cent of Canadian businesses, study says", *The Globe and Mail*, August 18, 2014, at http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 12

© 2015, CCH Canadian Limited

Given the seriousness of data security as a business issue, management, including the General Counsel, should be responsible for assessing a company's risks and developing an appropriate risk management policy.

Identifying a business's risk profile for loss arising from a privacy breach requires an analysis of a number of factors:

- ***Sector:*** Although any company that collects and stores its employees' or customers' personal information is exposed, recent Canadian statistics[47] suggest that the following sectors (in order of severity) are particularly at risk:
  - Telecommunications;
  - Financial (including banks, credit card companies, loan brokers, financial advisers, and related enterprises);
  - Sales/retail; and
  - Services.
- ***Type of Data:*** The data most often targeted by cyber criminals is intellectual property, followed by customer data.[48]
- ***Number of employees/customers:*** In general, companies with a large number of employees, companies that are significant users of social media, or companies that interact with a large number of customers, are particularly at risk. Employees who carry a proliferation of mobile devices, such as laptops, smart phones, iPads, USB drives, jump drives, media cards, tablets, and so on, containing sensitive information, represent one of the top concerns.[49] Industries that use credit or debit card processing, and that access financial or health information, are at greater risk.
- ***Smaller companies lacking robust preventative programs:*** Although contradictory to the comment above regarding higher risks being associated with larger companies, smaller companies are increasingly the subject of data breaches by cyber attackers and they may be particularly vulnerable as they often lack the resources to undertake as robust a preventative program as a larger company.[50] The results of the 2014 Ponemon global study show that companies are far more likely to have a small data breach than a mega breach.[51]
- ***High-profile companies:*** Businesses with high public profiles are more susceptible to organized crime for financial profit or risk of terrorist activity. Targeted criminal attacks pose a significant and most costly exposure (42% in a recent study).[52]
- ***Sharing of information with third parties:*** Companies that share personal information with third parties (such as outsourcers, contractors, consultants, and business partners) have a higher risk of a breach. Statistics show such breaches in the United States to be more costly than a breach by the company itself — averaging $43 more per compromised data record.[53]
- ***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. As noted by the Privacy Commissioner of Canada in her 2009 Annual Report, "Canada cannot function in isolation … Protecting privacy can no longer be done on a country-by-country basis — the international data flows are too great;

[47] Privacy Commissioner of Canada, *Annual Report to Parliament 2013*, June 2014, available at https://www.priv.gc.ca/information/ar/201214/2013_pipeda_e.pdf.

[48] Ponemon Institute, "Exposing the Cybersecurity Cracks: Canada," June 2014, at https://www.websense.com/assets/reports/report-ponemon-2014-part1-summary-canada-en.pdf.

[49] Ponemon Institute, *2013 State of the Endpoint*, December 5, 2012, available at http://www.ponemon.org/blog/2013-state-of-the-endpoint.

[50] "Should you Consider Cyber-Liability Insurance?", April 24, 2013, available at http://www3.cfo.com/article/2013/4/data-security_cyber-attacks-cybersecurity-liability-insurance-smb-growth-companies-risk-hogan-lovells.

[51] Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis, May 2014", at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded.

[52] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, May 2014, at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded.

[53] Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*, May 2013, available at https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 13

the technologies are evolving too rapidly; and the jurisdictional challenges are too daunting".[54]

Service agreements and contracts with customers in the United States typically obligate Canadian companies to comply with US security and privacy regulations. Compliance with foreign laws may also place a Canadian business in a position of non-compliance with Canadian privacy laws.[55]

¶43-708 Identifying Losses Associated with a Privacy Breach

Data breaches continue to be very costly for organizations. Results from the well-recognized US study by the Ponemon Institute in 2014[56] found the average global cost of a data breach to be $145 per record (compared to $201 for US companies), with the average total organizational cost amounting to $3.5 million. Malicious or criminal attacks caused 42 per cent of global data breaches in 2013, 30 per cent concerned a negligent employee or contractor, and 29 per cent involved system glitches. Heavily regulated industries (such as health care, education, pharmaceutical, and financial services) incurred costs that were substantially above the overall mean of $145 for other industries.

The Ponemon study showed that organizations with strong security postures, incident response plans, and chief information security officer positions experienced costs that were $14.14, $12.77, and $6.59, respectively, less than other organizations.

The following are some of the principal losses associated with privacy breaches that ought to be considered as part of a risk assessment and management program for privacy liability risk:

- ***Third-party liability:*** Losses that a company may incur as a result of harm to other individuals or entities include:
  - ***Compensation to clients or employees:*** For general damages and out-of-pocket costs.[57]
  - ***Compensation/subrogation to other entities:*** Compensation to third parties, such as downstream businesses or credit card companies, that incur losses associated with your company's privacy breach or damage to data or disablement of their computer system or website. Specific losses include:
    - damages for lost or stolen data, misappropriation of intellectual property or confidential business information;
    - issuing new payment cards and paying fraud expenses associated with compromised cards;
    - repairing damage to computer systems or electronic data; and
    - costs of interruption of service.
  - ***Contractual fines/penalties:*** Payment of fines and penalties arising out of a breach of contractually imposed industry-specific privacy standards, such as PCI DSS.[58]
  - ***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 resulting from a breach.

[54] Office of the Privacy Commissioner of Canada, "Annual Report to Parliament 2009", available at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.asp; and "Annual Report to Parliament 2010", available at http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.asp.

[55] 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 US-based Google's software system will force users into compliance with the US *Patriot Act*, which was passed in the wake of the September 2001 terrorist attacks and which gives US authorities sweeping powers to secretly view personal data held by US organizations. The move outraged Lakehead's faculty association, which filed a grievance against Lakehead's administration, alleging a breach of the collective agreement giving members a right to private communications.

[56] Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis", May 2014, at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid= SEL03027USEN&attachment= SEL03027USEN.PDF#loaded.

[57] These may include: (1) loss from bank or credit card accounts; (2) general damages for inconvenience and violation of privacy rights; (3) economic loss arising from time off work spent dealing with the incident; (4) compensatory damages for emotional harm, humiliation, or embarrassment; (5) costs incurred in gathering information about breached data; (6) funds expended in protecting personal information such as changing credit and debit accounts; cards and personal identifiers (such as social insurance numbers), and monitoring bank accounts, and credit card statements.

[58] See https://www.pcisecuritystandards.org/security_standards/index.php.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 14

© 2015, CCH Canadian Limited

– ***Defence:*** Legal costs incurred in response 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:

  – ***Privacy Commissioner of Canada:*** Costs associated with reporting breaches, responding to complaints, and defending investigations and proceedings before the Commissioner.[59]

  – ***Federal Court:*** Costs associated with the appeal of the Privacy Commissioner of Canada's findings, including damage awards for humiliation (with no cap on damage amount), fines, and penalties.

  – ***Criminal Code:*** Costs associated with defending criminal prosecutions, including legal costs, penal sanctions, and restitution awards.[60]

- ***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:

  – ***Response plan:*** Including: (1) discovery/detection (costs associated with the detection or discovery of the breach); (2) reporting (costs incurred in reporting the breach to all appropriate internal and regulatory personnel/bodies); and (3) 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: (1) credit report monitoring; (2) reissuance of new cards or accounts; (3) call centre and website to register complaints, provide information, and monitor activity; and (4) public relations.

  – ***Restoration/reconstruction:*** Including: (1) costs to restore or recreate lost or damaged information, including damaged IT systems; and (2) changes to internal processes.

  – ***Decline in revenue/business interruption:*** Lost business related to loss of trust and confidence by customers, negative reputational effects, and any interruption to business services.

  – ***Cyberextortion:*** Costs of extortion threats to commit an intentional computer attack against the company.

¶43-710 Best Practices To Reduce and Manage Privacy Breach Risk

¶43-710a Guidance from the Privacy Commissioner of Canada

In April 2013, the Office of the Privacy Commissioner of Canada and its counterparts in British Columbia and Alberta released a guidance document entitled, Getting Accountability Right with a Privacy Management Program, which outlines key steps that Canadian entities must take to be in compliance with Canadian privacy law and regulations.[61]

The following are recommended best practices to prevent and reduce costs associated with a data breach:

- ***Provide leadership:*** The organization should not leave data security to the IT department alone. Data security is a business issue.
- ***Educate and train employees:*** Most breaches are the result of human error. Educate and train employees as to how to handle confidential information.
- ***Encrypt data:*** Critical data, particularly mobile devices, should be encrypted.
- ***Develop and maintain a retention and destruction policy:*** Large databases of outdated information are often retained for no valuable

[59] These may include (1) legal defence costs; and (2) compliance with a regulator's recommendation — including improvement to safety practices and retention of a third-party auditor.

[60] RSC 1985, c. C-46.

[61] Available at https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 15

reason to the company, yet are a treasure trove for data thieves.

- ***Preventative measures:*** Conduct a more comprehensive analysis of privacy issues of a product before it is widely marketed and increase transparency by ensuring that customers are properly informed and consent to collection and disclosure of their information.
- ***Develop an incident response plan:*** The plan should include proper steps for customer notification. The data response team should include representatives from key groups within the company, including legal, IT, information security, human resources, public relations, and customer service.

¶43-710b Additional Risk Mitigation Measures

In addition, risk mitigation can be addressed through the steps outlined below:

- ***Identify and understand risks and adopt security measures:***
  - Identify the company's business risks;
  - Understand the exposures;
  - Review technical and information security policy safeguards;
  - Align company processes and protocols with relevant laws; and
  - Develop an appropriate action plan that includes the establishment of an effective privacy policy, disaster recovery and business continuity plans, mobile device protocols, employee training, and data classification standards.
- ***Contractual indemnity:*** If the company retains third-party service providers to perform services that allow access to your company's electronic systems or data:
  - Consider including in the service agreement contractual provisions that mandate that the service provider indemnify the entity for all losses arising from the loss or theft of personal information.
  - Consider contractually requiring the service provider to purchase appropriate insurance coverage and provide the company with the opportunity to review or approve such coverage.
- ***Insurance coverage:*** Conducting an audit of the 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 most likely will not be able to respond adequately, with the result that the company in breach may be left wholly or partially exposed.

¶43-712 Managing Privacy Risks Through Insurance

¶43-712a Privacy Liability Insurance Terminology

Terminology in this area of insurance may be confusing as many labels are used to market similar types of coverage, such as "privacy liability insurance", "network security liability insurance", "Internet media liability insurance", "cyber insurance", and "technology E&O", to name but a few.

Despite the differing labels, each provides somewhat similar (although certainly not identical) coverage for liability after a data breach. The term "privacy insurance" is used throughout this chapter to refer to all these products.

¶43-712b Integrating Privacy Liability Insurance into a Risk Management Program

Although insurance is not a substitute for proactive cybersecurity risk management, it is one of the tools available to allow a company to weather a storm if problems emerge. The Canadian insurance market has developed many new products in the past few years to specifically address emerging risks, but such products have yet to be wholeheartedly embraced. As a result, many companies faced with data or privacy breaches may be looking to their traditional insurance policies for coverage. In many cases they will be disappointed.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 16

© 2015, CCH Canadian Limited

- ***Key stages:*** A prudent risk management approach should include:
  - ***Insurance coverage audit:*** An audit of a company's existing insurance coverage;
  - ***Gap analysis:*** An analysis of any gaps in insurance coverage; and
  - ***Market review:*** A comprehensive review of the insurance market to ensure that appropriate protection is in place, in advance of a breach.
- ***Preliminary considerations:*** As a general guideline, the following points should be kept in mind:
  - ***Limitations of traditional insurance:*** Traditional insurance such as Property, Crime, Comprehensive General Liability, D&O, and E&O may, but may well not, respond to privacy breaches.
  - ***Variation in policy terms:*** Privacy-focused insurance products are available and differ widely. Beware of the fine print.
  - ***Extension versus stand-alone coverage:*** Privacy insurance can be purchased as extensions to existing policies or as stand-alone coverage. Stand-alone coverage will provide more comprehensive coverage with dedicated limits of liability for those risks.

    Some aspects of coverage (often first-party coverage) may be subject to a lower "sublimit" of coverage.
  - ***Tips for coverage negotiation:*** Successful negotiation and placement of this coverage requires identification and consideration of the company's risks, knowledge of the available coverage in the marketplace, and careful attention to the specific policy language.
  - ***Avoid coverage gaps and overlaps:*** Careful attention to a company's overall structure of an insurance program is necessary to avoid gaps and overlap between coverages.
  - ***Obtain expert advice:*** Expertise in auditing and understanding privacy insurance coverage should be obtained by in-house counsel from insurance brokers, lawyers, and/or consultants.

¶43-712c Understanding the Limitations on Coverage Under Traditional Insurance Policies

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.[62] Increasing judicial guidance is evolving from insurance coverage litigation, particularly in the United States, as companies with traditional policies seek to find coverage for cyber/privacy losses under policies whose language did not anticipate the types of exposures now arising.

This area of the law is anything but static. 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. Although reading and understanding insurance policies is not an easy task, and often best left to experts in that field, a general overview of the basic coverage under traditional policies is as follows:

- ***Property insurance policy:*** This kind of policy is generally not recommended for privacy risks:
  - ***Coverage for physical damage to tangible property:*** Property policies were designed for physical assets and physical perils and thus usually require physical damage to tangible property to trigger coverage.
  - ***Exclusion of "data":*** Property insurance policies typically exclude data from the meaning of tangible property.[63] 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" often include: (1) data erasure, destruction, corruption, misappropriation, or misinterpretation; (2) errors in creating,

[62] 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.

[63] "Data" is often defined to mean representations of information or concepts in any form.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 17

amending, entering, deleting, or using data; and (3) an inability to receive, transmit, or use data.

– ***Physical loss from data problems may be covered:*** 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.[64]

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 sublimits of coverage.

– ***Loss mitigation and management costs not covered:*** 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 intent to harm, and cover theft of money, securities, and tangible property. They do not typically 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:
  – ***Coverage only for physical damage to tangible property/bodily injury:*** The required trigger of physical damage to tangible property or bodily injury does not often occur in a privacy breach.
  – ***Exclusion of data:*** Tangible property often specifically excludes "electronic data", which is normally very broadly defined and includes such matters as information stored on computer software.
  – ***Limited coverage for privacy rights:*** Coverage for "personal injury" is generally limited to oral and written publication of confidential information which violates a person's right to privacy. Since hacking and other unauthorized disclosures of personal information may not involve any sort of intentional publication by the insured, there may be no coverage.

  Note that there is considerable litigation in the United States focusing on the meaning of "publication", and on the scope of an individual's "right to privacy" and thus these coverage questions are far from resolved.[65]

  – ***Gap for emotional distress coverage:*** 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.
  – ***Limitations on coverage for content beyond online advertising:*** "Advertising injury" coverage does not generally cover activities where the insured's products or services are not being promoted. With the evolution of websites, electronic chat rooms, bulletin boards, tweets, and blogs that provide information beyond advertising, not all content may be covered.
  – ***Loss mitigation and management costs not covered:*** 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 organization's directors and officers.
  – ***Organization not covered:*** Privacy breaches typically arise out of activities of the entity, and, under D&O insurance, the organization, if covered at all, would typically only have securities loss coverage.
  – ***Exclusions:*** Problematic exclusions would include those relating to property damage, intentional acts, and actions by one insured against another insured.
  – ***Examples of what may be covered:*** Some coverage may be available in respect of actions

[64] For example, damage to computer hardware arising from a fire may be covered although the loss of data information would not be covered.

[65] See *Zurich American Insurance Co. v. Sony Corp of America* Index Number: 651982/2011 (NY Sup Ct February 21 2014), which found no coverage under a CGL policy for litigation arising out of the hacking of Sony's PlayStation systems.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 18

© 2015, CCH Canadian Limited

against the directors and/or officers 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.
  - ***Coverage for damages out of covered professional service:*** 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.
  - ***Gaps in coverage under media policies:*** 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 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.

¶43-712d Highlights of Privacy and Network Security Insurance

The insurance market has been increasingly responsive to evolving privacy liability, with approximately 50 carriers offering some type of privacy-specific coverage today. Specially designed products, which 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. This growth has led the *New York Times* to call cyber insurance the "fastest growing niche in the [insurance] industry today."[66] 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 is 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 it is important to work with an insurer to craft unique and customized coverage that will be responsive to a business's specific risks.

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.
- ***Triggering the coverage:*** 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 fully mandated (unlike in the United States), it is important that the policy contain a trigger that is less restrictive than that contained in many US 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:***
  - ***Third-party liability:*** These policies typically cover third-party damages and claim expenses that arise out of claims brought by third parties after a data breach. They may also cover losses of information broader than personal information, including intellectual property or confidential business information. The cause of the loss may be a data breach (by intentional hacking or negli-

[66] Nicole Perlroth and Elizabeth A Harris, "Cyberattack Insurance a Challenge for Business", *The New York Times*, available at http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 19

gence), or a network breach, including transmission of malicious code or denial of third-party access to the insured's network, and other security threats to networks. It is desirable to have coverage extend to information in any format, including paper. The coverage usually includes amounts that 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, and potentially contractual fines such as under Payment Card Industry agreements.

– ***First-party liability:*** The policy will usually provide coverage for expenses incurred in attempting to mitigate damages as a result of a breach, and to repair/replace damaged data/systems including:

  • retention of a public relations firm and crisis management costs;

  • call centre and website expenses to handle inquiries from employees or customers;

  • credit/fraud monitoring costs;

  • costs involved in notifying customers or employees whose data has been compromised;

  • forensic investigation costs;

  • costs to recover/repair data/systems;

  • business interruption resulting from disabled operations;

  • reward payments made to informants for information which leads to conviction of person responsible for security breaches and/or extortion; and

  • extortion from cyber attackers who have stolen data.

Some policies will include access to service providers such as credit monitoring facilities, call centres, forensic accountants, law firms, and public relations and crisis management companies.

• ***Exclusions:*** 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, and 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.

– ***Shortcomings in security measures:*** Specific to privacy policies may be exclusions related to shortcomings in the insured's security measures noted in the underwriting process or known to the insured prior to policy inception.

• ***Key considerations:*** Given the differing wordings between insurance products in this area, it is impossible to provide a complete listing of policy terms. As noted previously, a thorough review of the policy with keen attention to detail is key to obtaining appropriate coverage. The following list highlights some areas of difference between insurance products in the market, which should be considered when analyzing appropriate solutions:

– Policy complexity;

– Coverage for actual and potential as well as electronic and hard data breaches;

– Claim venue (are regulatory proceedings covered?);

– Coverage for claims brought by or perpetrated by employees;

– Director and officer coverage innovations — the more the better — including severability, potential claim reporting, and final adjudication on fraud exclusion;

– Coverage for fines and penalties; and

– Global laws — how does the policy respond to breach of Canadian laws in order to comply with foreign laws?

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 20

© 2015, CCH Canadian Limited

¶43-712e Limits of Liability and Capacity

A common question asked by insureds is "how much coverage should I buy?" Unfortunately this is not capable of a quick, scientific answer. The upper limits of liability available in terms of worldwide capacity is approximately $300 million to $350 million per policy purchased, although retailers may find they are only able to secure a tower of up to $250 million in the aftermath of the Target breach. This would be provided by a number of different insurers with multi-layers of coverage stacked on top of each other. The first layer (the "primary policy") typically offers limits between $5 million and $25 million, with an average limit of $10 million. Most carriers offer a lower (sublimit) for first-party coverage related to privacy breaches.

- ***Determine risk exposure and conduct cost-benefit analysis:*** In order to make an informed decision on how much coverage to buy, the company needs to determine:
  - ***Risk exposure:*** What is the company's risk exposure?
  - ***Predicting loss:*** What amount of loss can be predicted?
  - ***Insurance protection:*** How much of the predicted loss does the company want to protect through insurance?

  A cost-benefit analysis is necessary.

¶43-712f Purchasing Coverage for Privacy Risks

- ***Application and audit:*** Many of the newer privacy policies have eliminated the need by companies to undergo lengthy audits and fill out complicated applications in order to obtain coverage.[67] Companies may be required to fill out an application (typically fairly simple) 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 typically does not affect the policy terms or pricing. A sample privacy policy application is at ¶43-746b.
- ***How underwriters define privacy risk:*** 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;
  - Use of social media and mobile devices;
  - 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; and
  - History of claims or breaches.

[67] This was 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).

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 21

¶43-740 PRECEDENTS/PRACTICAL TOOLS

¶43-742 Charts

Map of Canadian Privacy Laws

¶43-744 Checklists

¶43-744a Checklist: Reviewing and Developing a Privacy Liability Risk Management Program

- ***Provide leadership:*** Data security is a business issue and shouldn't be left to the IT department alone.
- ***Identify and understand risks:***
  - ***Business risks:*** Identify the company's business risks.
  - ***Exposures:*** Understand the exposures.
- **Adopt security measures and action plan:**
  - ***Review safeguards:*** Review technical and information security policy safeguards.
  - ***Ensure legal compliance:*** Align company processes and protocols with relevant laws.
- ***Develop an appropriate action plan that provides for the following:***
  - ***Privacy policy:*** Establish and maintain an effective privacy policy.
  - ***Disaster recovery and business continuity:*** Establish and maintain disaster recovery and business continuity plans.
  - ***Mobile device protocols:*** Establish and maintain mobile device protocols.
  - ***Education and training:*** Educate and train employees in the proper handling of confidential

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 22

© 2015, CCH Canadian Limited

information in order to reduce the risk of breaches arising from human error.

– ***Data classification:*** Establish and maintain data classification standards.

- ***Handle data appropriately:***

  – ***Encryption:*** Encrypt critical data, particularly on mobile devices.

  – ***Information retention and destruction:*** Develop and implement a data retention and destruction policy.

- ***Develop and use preventative measures:***

  – ***Analysis of issues:*** Conduct an analysis of privacy issues before a product/service is widely marketed.

  – ***Transparency:*** Ensure that customers are properly informed and consent to the collection and disclosure of their information.

- ***Develop an incident response plan:***

  – ***Customer notification:*** Include steps for customer notification of an incident.

  – ***Response team members:*** Include representatives from key groups within the company, including legal, IT, information security, human resources, public relations, and customer service.

- ***Review service agreements with third-party service providers:*** If your company retains third-party service providers to perform services that allow access to your company's electronic systems or data, consider:

  – ***Indemnification provisions:*** Contractual provisions in the service agreement mandating that the service provider indemnify the entity for all losses arising from the loss or theft of personal information.

  – ***Mandatory insurance coverage:*** Contractually requiring the service provider to purchase appropriate insurance coverage and provide the company with the opportunity to review or approve such coverage.

- ***Obtain/review insurance:***

  – ***Audit:*** Conduct an audit of the company's existing insurance program.

  – ***Gap analysis:*** Conduct a gap analysis to determine gaps in insurance coverage.

  – ***Market review:*** Conduct a comprehensive review of the insurance market to ensure that appropriate protection will be in place for your company in advance of a breach.

  – ***Specialized privacy liability insurance:*** Consider obtaining specialized privacy liability insurance coverage where traditional insurance products would fall short of responding adequately to a privacy breach.

¶43-744b Checklist: Responding to a Privacy Breach

Note: This checklist is derived from the "Privacy Breach Checklist" developed by the Office of the Privacy Commissioner of Canada.

- ***Describe the incident:***

  – What was the date of the incident?

  – When was the incident discovered?

  – How was the incident discovered?

  – What was the location of the incident?

  – What was the cause of the incident?

- ***Contain the breach and conduct preliminary assessment:***

  – Has the breach been contained (information recovery, computer system shut down, locks changed)?

  – Has an appropriate individual been designated to lead the initial investigation?

  – Does a breach response team need to be assembled?

    - If yes, who should be included (e.g., privacy officer, security officer, communications, risk management, legal)?

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 23

– Has the company determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?

– Does the breach appear to involve theft or other criminal activity?

• If yes, have the police been notified?

– Has the company ensured that evidence that may be necessary to investigate the breach has not been destroyed?

• ***Evaluate risks associated with the breach:***

– What personal information was involved?

• What personal information was involved (name, address, SIN, financial, medical)?

• What form was the personal information in (e.g., paper records, electronic database)?

• What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

– What was the cause and extent of the breach?

• Is there a risk of ongoing breaches or further exposure of the information?

• Can the personal information be used for fraudulent or other purposes?

• Was the information lost or stolen? If stolen, can it be determined whether the information was the target of the theft or not?

• Has the personal information been recovered?

• Is this a systemic problem or an isolated incident?

– How many individuals have been affected by the breach and who are they? Example: employees, contractors, public, clients, service providers, other organizations.

– Is there any foreseeable harm from the breach?

• What harm to the individuals could result from the breach (e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?

• Who has received the information, and what is the risk of further access, use, or disclosure?

• What harm could the organization suffer as a result of the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)?

• What harm could the public suffer as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

• ***Provide notification:***

– Should affected individuals be notified?

• What are the reasonable expectations of the individuals concerned?

• What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?

• Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?

• What is the ability of the individual to avoid or mitigate possible harm?

• What are the organization's legal and contractual obligations?

If you decide that affected individuals do not need to be notified, note your reasons.

– If affected individuals are to be notified, when and how will they be notified and who will notify them?

• What form of notification will you use (e.g., phone, letter, email, in person, website, media, etc.)?

• Who will notify the affected individuals? Do you need to involve another party?

• If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

– What should be included in the notification? Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal informa-

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 24

© 2015, CCH Canadian Limited

tion disclosed in the notification to what is necessary:

- Information about the incident and its timing in general terms.
- A description of the personal information involved in the breach.
- A general account of what your organization has done to control or reduce the harm.
- What your organization will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves.
- Sources of information designed to assist individuals in protecting against identity theft.
- Contact information of a department or individual within your organization who can answer questions or provide further information.
- Whether your organization has notified a privacy commissioner's office.
- Additional contact information to address any privacy concerns to your organization.
- Contact information for the appropriate privacy commissioner(s).

– Are there others who should be informed of the breach?

- Should any privacy commissioners' office be informed?
- Should the police or any other parties be informed? (This may include insurers; professional or other regulatory bodies; credit card companies; financial institutions; credit reporting agencies; third-party contractors; internal business units not previously advised of the privacy breach; and a union, or other employee bargaining unit.)

- ***Prevent Future Breaches***
  - What short- or long-term steps do you need to take to correct the situation (e.g., staff training policy, policy review or development, or audit)?

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 25

¶43-746 Policies and Other Sample Documents

¶43-746a Sample Privacy Network Policy

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®

DECLARATIONS

CHUBB INSURANCE COMPANY OF CANADA
Herein called the Company

Policy Number: [Formatted Policy Number]

NOTICE: SOLELY WITH RESPECT TO INSURING CLAUSE A, THIS IS A CLAIMS MADE POLICY, WHICH APPLIES ONLY TO "CLAIMS" FIRST MADE DURING THE "POLICY PERIOD", OR AN APPLICABLE EXTENDED REPORTING PERIOD. THE LIMIT OF LIABILITY TO PAY "LOSS" WILL BE REDUCED, AND MAY BE EXHAUSTED, BY "DEFENCE COSTS" AND "DEFENCE COSTS" WILL BE APPLIED AGAINST THE RETENTION AMOUNT. IN NO EVENT WILL THE COMPANY BE LIABLE FOR "DEFENCE COSTS" OR ANY OTHER "LOSS" IN EXCESS OF THE APPLICABLE LIMIT OF LIABILITY. PLEASE READ THE ENTIRE POLICY CAREFULLY.

Item 1. **PARENT ORGANIZATION**

[Name]
[Address]

Item 2. **POLICY PERIOD**

Inception Date [Inception Date]

Expiration Date [Expiration Date]

At 12:01 A.M. standard time at the Address in ITEM 1

Item 3. **AGGREGATE LIMIT OF LIABILITY EACH POLICY PERIOD**

$ [Aggregate Limit of Liability]

Item 4. **LIMITS OF LIABILITY AND RETENTION AMOUNTS**

If **"NOT COVERED"** is inserted opposite any specified INSURING CLAUSE, such INSURING CLAUSE and any other reference to such INSURING CLAUSE in this Policy shall be deemed to be deleted.

	Insuring Clause	Each Claim Limit of Liability	Retention Amount
(A)	Cyber Liability	$ [Limit of Liability1]	$ [Retention1]

	Additional Insuring Clause	Single Expense Limit of Liability	Retention Amount
(B)	Privacy Notification Expenses	$ [Limit of Liability2]	$ [Retention2]
(C)(1)	Crisis Management Expenses	$ [Limit of Liability3]	$ [Retention3]
(C)(2)	Reward Expenses	$ [Limit of Liability4]	$ [Retention4]
(D)	E-Business Interruption and Extra Expenses	$ [Limit of Liability5]	$ [Retention5]
(E)	E-Theft Loss	$ [Limit of Liability6]	$ [Retention6]
(F)	E-Communication Loss	$ [Limit of Liability7]	$ [Retention7]
(G)	E-Threat Expenses	$ [Limit of Liability8]	$ [Retention8]
(H)	E-Vandalism Expenses	$ [Limit of Liability9]	$ [Retention9]

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 26

© 2015, CCH Canadian Limited

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®

Item 5	**COINSURANCE PERCENT:**	[Insert Percent Figure1] %
Item 6	**EXTENDED REPORTING PERIOD:**	
	(A) Additional Premium:	[Insert Percent Figure2] % of the Annualized Premium for the expiring **Policy Period**
	(B) Additional Period	[Insert Time Grant]
Item 7	**RETROACTIVE DATE:**	[Retroactive Date]
Item 8	**PENDING OR PRIOR DATE:**	[PPL Date]

In witness whereof, the Company issuing this Policy has caused this Policy to be signed by its authorized officers, but it shall not be valid unless also signed by an authorized representative of the Company.

CHUBB INSURANCE COMPANY OF CANADA

President

Date: [Issue Date]

Authorized Representative

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 27

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®

In consideration of payment of the premium and subject to the Declarations, limitations, conditions, provisions and other terms of this Policy, the Company and the **Insured** agree as follows:

I. INSURING CLAUSES

A. CYBER LIABILITY

The Company shall pay **Loss** on behalf of an **Insured** on account of any **Claim** first made against such **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for **Injury**.

B. PRIVACY NOTIFICATION EXPENSES

The Company shall pay **Privacy Notification Expenses** incurred by an **Insured** resulting from **Disclosure Injury** or **Reputational Injury**.

C. CRISIS MANAGEMENT AND REWARD EXPENSES

The Company shall pay **Crisis Management Expenses** and **Reward Expenses** incurred by an **Insured** and directly arising out of **Injury** covered under Insuring Clause A and/or **Expense** or **Loss** covered under Insuring Clauses D, E, F, G or H.

D. E-BUSINESS INTERRUPTION AND EXTRA EXPENSES

The Company shall pay:

a. The loss of **Business Income** an **Insured** incurs during the **Period of Recovery of Services** due to the actual impairment or denial of **Operations** resulting directly from **Fraudulent Access or Transmission**, and

b. **Extra Expenses** an **Insured** incurs during the **Period of Recovery of Services** due to the actual or potential impairment or denial of **Operations** resulting directly from **Fraudulent Access or Transmission;**

when the **Fraudulent Access or Transmission** causes an actual or potential impairment or denial of **Operations** during the **Policy Period**.

E. E-THEFT LOSS

The Company shall pay **E-Theft Loss** first discovered during the **Policy Period**.

F. E-COMMUNICATIONS LOSS

The Company shall pay **E-Communications Loss** first discovered during the **Policy Period**.

G. E-THREAT EXPENSES

The Company shall pay **E-Threat Expenses** resulting directly from an **Insured** having surrendered any funds or property to a natural person who makes a **Threat** directly to an **Insured** during the **Policy Period**.

H. E-VANDALISM EXPENSES

The Company shall pay **E-Vandalism Expenses** an **Insured** incurs resulting directly from the alteration, damage, deletion, or destruction of any **Data** which is owned by an **Insured** or for which an **Insured** is legally liable when first discovered during the **Policy Period**.

II. DEFINITIONS

Application means all signed applications, and any attachments, information, warranty, or other materials submitted in connection with such applications or referenced or incorporated therein, submitted by or on behalf of the **Insureds** to the Company for this Policy or for any policy of which this Policy is a direct or indirect renewal or replacement. **Application** shall also include any cyber security questionnaires and cyber security risk matrixes submitted in connection with the underwriting analysis. All such applications, attachments, materials, questionnaires and matrixes are deemed attached to, incorporated into and made a part of this Policy.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 28

© 2015, CCH Canadian Limited

Benefit Plan means any **Government Benefit Program,** Canadian Employee Benefit Plan, Registered Pension Plan, Group Sickness or Accident Insurance Plan, Private Health Service Plan, Supplementary Unemployment Benefit Plan, Deferred Profit-Sharing Plan, Employees' Profit Sharing Plan, Sickness or Accident Insurance Plan, Disability Insurance Plan, Income Maintenance Insurance Plan, Vacation Pay Trust, Employee Trusts, Retirement Compensation Arrangement or Salary Deferral Arrangement so defined in the Income Tax Act of Canada, S.C. 1985 Ch 1, including any rules or regulations there under, as amended, or any comparable **Foreign** law in respect of employee benefits.

Business Income means:

A. net profit or loss that would have been earned or incurred before income taxes; and

B. an **Insured's** continuing normal operating and payroll expenses.

Business Income does not mean bank interest or investment income.

Canadian Privacy Law means the provisions of the Personal Information Protection and Electronic Documents Act, S.C. 2000, Ch. C-5, including any rules or regulations there under, as amended, or pursuant to the same or similar provisions of any legislation, rules or regulations in each of the provinces or territories of Canada, as amended or as applicable; or any similar applicable **Foreign** law.

Canadian Securities Law means the Securities Act of Ontario, R.S.O. 1990 Chapter S.5, including any rules or regulations there under, as amended, or pursuant to the same or similar provisions of any legislation, rules or regulations in each of the provinces or territories of Canada, as amended or as applicable; or any similar applicable **Foreign** law.

Claim means:

A. any of the following:

1. a written demand or written request for monetary damages or non-monetary relief;

2. a written demand for arbitration;

3. a civil proceeding commenced by the service of a statement of claim, complaint or similar pleading; or

4. a criminal proceeding commenced by return or service of an indictment, summons to appear, information or similar document

against an **Insured** for an **Injury**, including any appeal there from; or

B. a written request received by an **Insured** to toll or waive a limitation period relating to a potential **Claim** as described in paragraph A. above.

Except as may otherwise be provided in Section VIII, Extended Reporting Period, Section X, Retention Amount And Coinsurance, or Section XI, Reporting, a **Claim** will be deemed to have been first made when such **Claim** is commenced as set forth in this definition, or, in the case of a written demand or written request, including but not limited to a demand for arbitration, when such demand or request is first received by an **Insured**.

Common Law Partner means any natural person qualifying as a common law or domestic partner under the provisions of any applicable federal, provincial, territorial, state, local or **Foreign** law or under the provisions of any formal program established by the **Insured Organization**.

Communication means an electronic record or message created, generated, sent, communicated, received or stored by electronic means that is capable of retention by the recipient at the time of receipt, including a telefacsimile transmission or e-mail, and that was transmitted or purported to have been transmitted through a **Network**.

Computer means a device or group of devices that by manipulation of electronic, magnetic, optical or electromechanical impulses pursuant to a computer program can perform operations on **Data**.

Conduit Injury means injury sustained or allegedly sustained by a **Person** because a **System** cannot be used, or is impaired, resulting directly from:

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 29

A. a **Cyber-attack** into an **Insured's System**, provided such **Cyber-attack** was then received into a third party's **System**; or

B. a natural person who has accessed a **System** without authorization, through an **Insured's System**,

provided such transmission or access occurred on or after the **Retroactive Date** and before the end of the **Policy Period.**

Content Injury means injury sustained or allegedly sustained by a **Person** because the actual or alleged infringement of:

A. a collective mark, service mark, or other trademarked name, slogan, symbol or title;

B. a copyright;

C. the name of a product, service, or organization; or

D. the title of an artistic or literary work,

resulting directly from **Cyber Activities** of an **Insured**, provided that the **Cyber Activities** that caused or allegedly caused the **Content Injury** first occurred on or after the **Retroactive Date** and before the end of the **Policy Period**.

Crisis Management Expense means the reasonable and necessary cost of:

A. retaining, for a stipulated period of time with the prior approval of the Company:

1. independent legal counsel;

2. information security forensic investigators;

3. public relations consultants; or

B. advertising and public relations media and activities.

Customer means a **Person** that:

A. is applying for, or requesting, an **Insured Organization's** products or services;

B. has applied for, or has requested, an **Insured Organization's** products or services; or

C. is using, or has used, an **Insured Organization's** products or services.

Cyber Activities means the electronic display, electronic transmission, or electronic dissemination of information through a **Network** or through an **Insured's System**.

Cyber-attack means the transmission of fraudulent or unauthorized **Data** that is designed to modify, alter, damage, destroy, delete, record or transmit information within a **System** without authorization, including **Data** that is self-replicating or self-propagating and is designed to contaminate other computer programs or legitimate computer **Data**, consume computer resources or in some fashion usurp the normal operation of a **System**.

Data means a representation of information, knowledge, facts, concepts, or instructions which are being processed or have been processed in a **Computer**.

Defence Costs means that part of **Loss** consisting of reasonable costs, charges, fees (including but not limited to legal and experts' fees) and expenses (other than regular or overtime wages, salaries, fees or benefits of the directors, officers or employees of an **Insured Organization**) incurred in defending any **Claim**, and the premium for appeal, attachment or similar bonds.

Disclosure Injury means injury sustained or allegedly sustained by a natural person because of the potential or actual unauthorized access to such natural person's **Record** by another **Person** when such access:

A. occurs on or after the **Retroactive Date** and before the end of the **Policy Period**; and

B. results directly from:

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 30

© 2015, CCH Canadian Limited

1. a **Cyber-attack** into a **System** owned by an **Insured Organization**; or

2. a natural person who has gained unauthorized access to, or has exceeded authorized access to a **System** or **System Output** owned by:

   i. an **Insured Organization**; or

   ii. an organization that is authorized by an **Insured** through a written agreement to process, hold or store **Records** for an **Insured**.

E-Communications Loss means loss resulting directly from a **Customer**, automated clearing house, custodian, or financial institution having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value on the faith of any fraudulent **Communication** purporting to have been directed by an **Insured** to any of the foregoing for the purpose of initiating, authorizing or acknowledging the transfer, payment, delivery or receipt of funds or property, but which **Communication** was either not sent by an **Insured** or was fraudulently modified during electronic transmission and for which loss an **Insured** is held to be legally liable.

E-Theft Loss means loss resulting directly from an **Insured** having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value due to the fraudulent input of **Data** either directly into an **Insured's System** or through a **Network** into an **Insured's System**.

E-Threat Expenses means:

A. funds or property an **Insured** surrenders and any of the following expenses set forth below incurred by an **Insured**:

   1. reasonable fees and expenses of any independent negotiator or consultant;

   2. reasonable travel and accommodation expenses; or

   3. any other reasonable expense with the Company's prior written approval; or

B. loss resulting directly from the actual destruction, disappearance, confiscation or wrongful abstraction of funds or property intended as an extortion payment, while being held or conveyed by any **Person** duly authorized by an **Insured** to have custody of such funds or property,

solely and directly as a result of a **Threat** that would constitute an **Expense** under Insuring Clause G.

E-Vandalism Expenses means the cost of the blank media and the cost of labour for the actual transcription or copying of **Data** or **Media** furnished by an **Insured** in order to reproduce such **Data** or replace such **Media** from others of the same kind or quality.

Employee Benefit Plan means any plan so defined in the Income Tax Act of Canada S.C. 1985 Ch. 1, including any rules or regulations there under, as amended.

ERISA means the Employee Retirement Income Security Act of 1974, the Pension Protection Act of 2006, both of the United States of America, both including any rules or regulations promulgated there under, both as amended; and any similar common or statutory law anywhere in the world, including any rules or regulations promulgated under any such Acts or laws.

Exceeded Authorized Access means to access an **Insured's System** with authorization but to use such access to perform unauthorized fraudulent operations, including the fraudulent input of **Data**.

Expense means **Privacy Notification Expenses**, **Crisis Management and Reward Expenses**, **E-Business Interruption and Extra Expenses**, **E-Theft Loss**, **E-Communications Loss**, **E-Threat Expenses**, or **E-Vandalism Expenses.**

Extra Expenses means reasonable expenses an **Insured** incurs in an attempt to continue **Operations** that are over and above the expenses such **Insured** would have normally incurred. **Extra Expenses** do not include any costs of updating, upgrading or remediation of an **Insured's System** that are not otherwise covered under this Policy.

Financial Impairment means:

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 31

A. in Canada, the status of the **Parent Organization** resulting its financial position as a "debtor" as that term is defined and used in Canada within the provisions of the Canadian Bankruptcy and Insolvency Act, rules, regulations, orders and orders in council promulgated there under and amendments thereto, and, without limiting the generality of the foregoing shall occur when any receiver, conservator, liquidator, trustee, sequestrator or similar official has been appointed by a federal, provincial or territorial court , agency or official or by a creditor to take control of, supervise, manage or liquidate the **Parent Organization;** or a reorganization proceeding relating to the **Parent Organization** has been brought in Canada under the Companies' Creditors Arrangement Act, rules, regulations, orders, and orders in council promulgated there under and amendments thereto; or

B. in any jurisdiction other than Canada means the status of the **Parent Organization** resulting from the appointment by any state, provincial, territorial or federal official, agency or court of any receiver, conservator, liquidator, trustee, rehabilitator or similar official to take control of, supervise, manage or liquidate such entity.

Foreign means any jurisdiction outside of Canada.

Fraudulent Access or Transmission means that a **Person** has:

A. fraudulently accessed an **Insured's System** without authorization;

B. **Exceeded Authorized Access**; or

C. launched a **Cyber-attack** into an **Insured's System**.

Government Benefit Program means any **Benefit Plan** created by statute, of which the capital is administered and the contingent liabilities assumed by a government or governments or agency thereof, including without limitation workers compensation, unemployment, social security and disability benefit programs.

Impaired Access Injury means injury sustained or allegedly sustained by a **Customer** who is authorized by an **Insured Organization** to access an **Insured's System**, because such access has been impaired or denied, resulting directly from **Fraudulent Access or Transmission**, provided such **Fraudulent Access or Transmission** occurred on or after the **Retroactive Date** and before the end of the **Policy Period**.

Informant means any natural person providing information solely in return for monetary payment paid or promised by an **Insured**.

Injury means **Conduit Injury, Content Injury**, **Disclosure Injury, Impaired Access Injury** or **Reputational Injury**.

Insured means any **Insured Organization** and any **Insured Person**.

Insured Organization means the **Parent Organization** and any **Subsidiary**.

Insured Person means any natural person, who was, now is, or shall become a director or officer (or equivalent position of the foregoing) or employee of an **Insured Organization**, but only while active within the scope of his or her duties as such.

Intellectual Property Law or Right means any:

A. certification mark, collective mark, copyright, patent, service mark, or trademark;

B. right to, or judicial or statutory law recognizing an interest in, any trade secret or confidential or proprietary information;

C. other right to, or judicial or statutory law recognizing an interest in, any expression, idea, likeness, name, slogan, style of doing business, symbol, title, trade dress or other intellectual property; or

D. other judicial or statutory law concerning piracy, unfair competition or other similar practices.

Internet means a group of connected networks that allow access to an **Insured's System** through service providers using telephone service, digital subscriber lines, integrated service digital network lines, cable modem access or similar transfer mediums.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 32

© 2015, CCH Canadian Limited

Loss means the amount that an **Insured** becomes legally obligated to pay as a result of any covered **Claim**, including but not limited to damages (including punitive or exemplary damages if and to the extent that such punitive or exemplary damages are insurable under the law of the jurisdiction most favourable to the insurability of such damages, provided such jurisdiction has a substantial relationship to the relevant **Insured**, to the Company, or to the **Claim** giving rise to the damages), judgments, settlements, pre-judgment and post-judgment interest and **Defence Costs**. **Loss** does not include:

A. any consideration owed or paid in connection with any **Insured's** goods, products or services, including but not limited to any restitution, reduction, disgorgement or return of any payments, charges or fees;

B. any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**;

C. any costs or expenses incurred to replace, upgrade, update, improve, or maintain a **System**;

D. any costs incurred by any **Insured** to comply with any order for injunctive or other non-monetary relief, or to comply with an agreement to provide such relief;

E. any amount incurred by any **Insured** in the defence or investigation of any action, proceeding, demand or request that is not then a **Claim** even if such matter subsequently gives rise to a **Claim**;

F. taxes, fines, penalties (except as provided above with respect to punitive or exemplary damages under Insuring Clause A), liquidated damages or the multiple portion of any multiplied damage award; or

G. any amount not insurable under the law pursuant to which this Policy is construed.

Media means objects on which **Data** can be stored so that it can be read, retrieved or processed by a **Computer**. **Media** does not mean paper.

Network means any and all services provided by or through the facilities of any electronic or computer communication system, including Canadian Payments Association Clearing House System, Fedwire, Clearing House Interbank Payment System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT) and similar automated inter-bank communication systems, automated teller machines, point of sale terminals, and other similar operating systems and includes any shared networks, **Internet** access facilities, or other similar facilities for such systems including any of those used in **Foreign** jurisdictions, in which an **Insured** participates, allowing the input, output, examination, or transfer of **Data** or programs from one computer to an **Insured's Computer**.

Operations means an **Insured's** business activities.

Parent Organization means the **Person** designated in Item 1 of the Declarations.

Period of Recovery of Services:

A. begins:

1. for **Extra Expenses**, immediately after the actual or potential impairment or denial of **Operations** occurs; and

2. for the loss of **Business Income**, twenty-four (24) business hours after the actual impairment or denial of **Operations** occurs; and

B. will continue until the earlier of the following:

1. the date **Operations** are restored, with due diligence and dispatch, to the condition that would have existed had there been no impairment or denial; or

2. sixty (60) days after the date an **Insured's Services** are fully restored, with due diligence and dispatch, to the level that would have existed had there been no impairment or denial.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 33

The expiration date of this Policy will not cut short the **Period of Recovery of Services**.

Person means a natural person or an organization.

Policy Period means the period of time specified in Item 2 of the Declarations, subject to prior termination in accordance with Section XXIII, Termination of Policy. If this period is less than or greater than one year, then the Limits of Liability specified in the Declarations shall be the Company's maximum limit of liability under this Policy for such period.

Pollutants means:

A. any substance located anywhere in the world exhibiting any hazardous characteristics as defined by, or identified on a list of hazardous substances issued under the Canadian Environmental Protection Act, as amended, or by the United States Environmental Protection Agency or any federal, provincial, territorial, state, county, municipality or locality or **Foreign** counterpart thereof, including, without limitation, solids, liquids, gaseous or thermal irritants, contaminants or smoke, vapour, soot, fumes, acids, alkalis, chemicals or waste materials; or

B. any other air emission, odour, waste water, oil or oil products, infectious or medical waste, asbestos or asbestos products or any noise.

Privacy Notification Expenses means the reasonable and necessary cost of notifying those **Persons** who may be directly affected by the potential or actual unauthorized access of a **Record**; and

A. changing such **Person's** account numbers, other identification numbers and security codes; and

B. providing such **Persons**, for a stipulated period of time and with the prior approval of the Company, with credit monitoring or other similar services that may help protect them against the fraudulent use of the **Record**.

Record means a natural person's first name or first initial and last name, in combination with:

A. their social insurance number, social security number, driver's license number or other personal identification number (including an employee identification number or student identification number);

B. their financial account number (including a bank account number, retirement account number, or healthcare spending account number);

C. their credit, debit or payment card number;

D. any information related to their employment by an **Insured Organization**; or

E. any individually identifiable health information held by an **Insured Organization**, pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or any similar provision under **Canadian Privacy Law,**

when any of the information in "A" through "E" above is intended by an **Insured Organization** to be accessible only by **Persons** it has specifically authorized to have such access.

Related Claims means all **Claims** based upon, arising from, or in consequence of the same or related facts, circumstances, situations, transactions or events or the same or related series of facts, circumstances, situations, transactions or events.

Reputational Injury means injury sustained or allegedly sustained by a **Person** because of an actual or alleged:

A. disparagement of such organization's products or services;

B. libel or slander of such natural person; or

C. violation of such **Person's** rights of privacy or publicity,

resulting directly from **Cyber Activities** of an **Insured**, provided that the **Cyber Activities** that caused or allegedly caused the **Reputational Injury** first occurred on or after the **Retroactive Date** and before the end of the **Policy Period**.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 34

© 2015, CCH Canadian Limited

Retroactive Date means the date set forth in Item 7 of the Declarations, provided that if no date is set forth in Item 7, then the **Retroactive Date** shall be the inception date of this Policy.

Reward Expenses means the reasonable amount paid by an **Insured**, with the prior approval of the Company, to an **Informant** for information not otherwise available which leads to the arrest and conviction of persons responsible for a **Cyber-attack**, **Fraudulent Access or Transmission**, or a **Threat** otherwise covered under this Policy.

Services means computer time, data processing, or storage functions or other uses of an **Insured's System**.

Single Expense means, with respect to Insuring Clauses B through H, all covered expense or loss resulting from:

A. any one act or series of related acts on the part of any natural person resulting in damage or destruction of **Data** or **Media**;

B. any one act or series of related acts which impairs or denies an **Insured's Services**;

C. all **Threats** related by a common committed, attempted or threatened wrongful act or made contemporaneously against the same **Insured**;

D. all loss of property and other consideration actually surrendered as ransom and extortion payments arising from one **Threat** or a series of related **Threats**;

E. all expenses arising from one **Threat** or a series of related **Threats**;

F. all acts, other than those specified above, caused by any person or in which such person is implicated; or

G. any one event not specified above.

Subsidiary means any organization, at or prior to the inception date of the Policy, in which more than fifty percent (50%) of the outstanding securities or voting rights representing the present right to vote for election of directors of such organization are owned, directly or indirectly, in any combination, by one or more **Insured Organizations**.

System means a **Computer**; and

A. all input, output, processing, storage and communication devices controlled, supervised or accessed by the operating systems that are proprietary to, or licensed to, the owner of the **Computer**; and

B. **Media**.

System Output means a tangible substance on which one or more **Records** are printed from a **System**.

Threat means a declaration made by a natural person that he or she has gained access or alleges to have gained access to an **Insured's System** and intends to:

A. cause an **Insured** to transfer, pay or deliver any funds or property using an **Insured's System**;

B. sell or disclose a **Record** to another person;

C. alter, damage or destroy an **Insured's Data** while stored within an **Insured's System**;

D. alter, damage, or destroy an **Insured's Data** through a **Cyber-attack**; or

E. impair or deny an **Insured's Services**,

where there exists a demand for an extortion payment or a series of such payments as condition for the mitigation or removal of such **Threat**.

III. EXCLUSIONS:

A. With respect to Insuring Clause A, the Company shall not be liable for **Loss** on account of any **Claim**:

1. based upon, arising from, or in consequence of any demand, suit or other proceeding pending against, or order, decree or judgment entered for or against any **Insured**, on or prior to the

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 35

Pending or Prior Date set forth in Item 8 of the Declarations, or the same or substantially the same fact, circumstance, situation, transaction, event, act or omission underlying or alleged therein;

2. for any actual or alleged violation by any **Insured** of the:

   a. statutory or common law responsibilities, obligations or duties imposed on fiduciaries by any **Benefit Plan**; or

   b. responsibilities, obligations or duties imposed on fiduciaries by **ERISA**;

3. brought or maintained by or on behalf of a natural person who is a director, chairman, chief executive officer, president or chief operating officer of any **Insured Organization** or who holds a similar title or position within any **Insured Organization**;

4. based upon, arising from, or in consequence of any actual or alleged infringement of, violation of or assertion of any right to or interest in a patent or trade secret by any **Insured**;

5. based upon, arising from, or in consequence of any claim or proceeding brought by or on behalf of any:

   a. federal, provincial, territorial, state, or local government agency or authority; or

   b. licensing or regulatory organization;

6. based upon, arising from, or in consequence of any electronic, oral, written, or other publication of information, by, on behalf of, or with the consent of any **Insured**;

   a. with the knowledge of its falsity; or

   b. if a reasonable person in the circumstances of such **Insured** would have known such to be false;

7. based upon, arising from, or in consequence of the failure of goods, products, or services to conform with any electronic, oral, written, or other representation or warranty with respect to durability, fitness, performance, quality, or use;

8. for **Content Injury** or **Reputational Injury** sustained by any **Person** that:

   a. creates, designs, develops, or provides any content, material, or services for any **Insured**; or

   b. is an assign or heir of any **Person** described in Exclusion A.8.a. above;

   provided that this Exclusion A.8. applies regardless of whether such content, material, or service was jointly created, designed, developed, or provided by any **Insured**;

9. for **Content Injury** or **Reputational Injury** that is based upon, arises from, or in consequence of any:

   a. distribution or sale of, or offer to distribute or sell, any good, product, or service; or

   b. other use of any good, product, or service,

   that actually or allegedly infringes or violates any **Intellectual Property Law or Right** relating to the appearance, design or function of any good, product, or service;

10. based upon, arising from, or in consequence of:

    a. controlling, creating, designing, or developing any third party's Web site;

    b. controlling, creating, designing, developing, determining, or providing the content of material of any third party's Web site; or

    c. controlling, facilitating, or providing, or failing to control, facilitate, or provide, access to the **Internet**; or

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 36

© 2015, CCH Canadian Limited

11. based upon, arising from, or in consequence of any actual or alleged infringement of, violation of, or assertion of any right to or interest in any:

    a. software or its source content or material;

    b. computer code or its source content or material; or

    c. expression, method, or process designed to control or facilitate any operation or other use of a **Computer** or automated system.

B. With respect to Insuring Clauses B through H, the Company shall not be liable for:

1. any consideration owed or paid in connection with any **Insured's** goods, products or services, including but not limited to any restitution, reduction, disgorgement or return of any payments, charges or fees;

2. any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**;

3. any loss, costs or expenses any **Insured** agrees to incur or incurs on behalf of another **Person** when such **Insured** is not obligated to incur such loss, costs or expenses under the Uniform Commercial Code or any other law, statute, rule or code anywhere in the world, including the rules or codes of any clearing or similar organization; provided that this Exclusion B.3. does not apply to Insuring Clauses B, C or D;

4. any costs, fees or expenses incurred or paid by any **Insured** in establishing the existence of or amount of loss;

5. any costs or expenses incurred to replace, upgrade, update, improve, or maintain a **System**;

6. any costs incurred by any **Insured** to comply with any order for injunctive or other non-monetary relief, or to comply with an agreement to provide such relief;

7. taxes, fines, penalties, liquidated damages or the multiple portion of any multiplied damage award;

8. any potential income, including but not limited to interest and dividends not realized by any **Insured** or any **Customer** of any **Insured**; provided that this Exclusion B.8. shall not apply to loss of **Business Income** otherwise covered under Insuring Clause D.

C. With respect to Insuring Clauses D through H, the Company shall not be liable for any **Expense:**

1. caused by an employee of any **Insured**; provided that this Exclusion C.1. shall not apply to Insuring Clauses D, G, or H;

2. resulting directly or indirectly from written instruction or advice, other than a telefacsimile or e-mail; or telegraphic or cable instruction or advice, or instruction or advice by voice over the telephone;

3. resulting directly or indirectly from forged, altered or fraudulent negotiable instruments, securities, documents or written instruments used as source documentation in the preparation of **Data**;

4. based upon, or directly or indirectly arising out of or resulting from an indirect or consequential loss of any nature; provided that this Exclusion C.4. shall not apply to Insuring Clause D;

5. relating to negotiable instruments, securities, documents or written instruments except as converted to **Data** and then only in that converted form; or

6. resulting from mechanical failure, faulty construction, error in design, latent defect, wear or tear, gradual deterioration, electrical disturbance, **Media** failure or breakdown or any malfunction or error in programming or error or omission in processing.

D. With respect to all Insuring Clauses, the Company shall not be liable for any **Loss** on account of any **Claim**, or for any **Expense**:

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 37

1. based upon, arising from, or in consequence of any fact, circumstance, situation, transaction, event, act or omission that was the subject of any notice given under any policy or coverage section of which this Policy is a direct or indirect renewal or replacement;

2. based upon, arising from or in consequence of the committing in fact of any deliberately criminal, fraudulent or dishonest act or omission or any wilful violation of any statute or regulation by, on behalf of, or with the consent of any **Insured**, as evidenced by:

   a. any written statement or written document by any **Insured**; or

   b. any judgment, award, order, decree or ruling or equivalent determination in any judicial, administrative or alternative dispute resolution proceeding;

3. based upon, arising from or in consequence of any:

   a. breach of contract or agreement; or

   b. liability assumed by any **Insured** under any contract or agreement,

   provided that this Exclusion D.3.a. shall not apply to **Conduit Injury**, **Impaired Access Injury** or **Disclosure Injury** or to the extent that an **Insured** would have been liable in the absence of the contract or agreement;

4. based upon, arising from, or in consequence of:

   a. any actual, alleged, or threatened exposure to, or generation, storage, transportation, discharge, emission, release, dispersal, escape, treatment, removal or disposal of any **Pollutants**;

   b. any regulation, order, direction or requests to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize any **Pollutants**, or any action taken in contemplation or anticipation of any such regulation, order, direction or request;

   c. any nuclear fission, fusion or radioactivity; or

   d. any riot or civil commotion, outside of Canada or the United States of America, or any military, naval or usurped power, war or insurrection;

5. for bodily injury, mental anguish, emotional distress (except mental anguish and emotional distress resulting from **Disclosure Injury** or **Reputational Injury**), sickness, disease or death of any person or damage to, destruction of or loss of use of any tangible property whether or not it is damaged or destroyed;

6. based upon, or directly or indirectly arising out of, or resulting from any function or activity as a receiver, trustee in bankruptcy, conservator or assignee for the benefit of creditors;

7. based upon, or directly or indirectly arising out of, or resulting from:

   a. the underwriting, securitizing, syndicating, promoting, or market making (as defined in Section 3 (a) (38) of the Securities Exchange Act of 1934 as amended, or in **Canadian Securities Law**) of any debt or equity security or other evidence of indebtedness, or any loan or other extension of credit, or any other similar investment banking activity;

   b. any actual, attempted or threatened merger, acquisition, divestiture, tender offer, proxy contest, leveraged buy-out, going private transaction, insolvency proceeding, reorganization, capital restructuring, recapitalization, spin-off, primary or secondary offering of debt or equity securities or other evidence of indebtedness, dissolution or sale of all or substantially all of the assets or stock of a business entity or any effort to raise or furnish capital or financing for any enterprise or entity;

   c. a fairness opinion;

   d. the valuation of any assets or business entity; or

   e. any acquisition or sale of securities by any **Insured** for their own account,

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 38

© 2015, CCH Canadian Limited

or any disclosure requirements in connection with any of the foregoing.

IV. SEVERABILITY OF EXCLUSIONS

For the purposes of determining the applicability of Section III. Exclusions A.6. and D.2.:

A. no fact pertaining to or knowledge possessed by any **Insured Person** shall be imputed to any other **Insured Person** to determine if coverage is available; and

B. only facts pertaining to or knowledge possessed by an **Insured Organization's** chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing shall be imputed to such **Insured Organization** to determine if coverage is available.

V. SPOUSES, COMMON LAW PARTNERS, ESTATES AND LEGAL REPRESENTATIVES

Coverage shall extend to **Claims** for the covered acts, errors or omissions of an **Insured Person** made against:

A. the lawful spouse or **Common Law Partner** of such **Insured Person**, if named as a co-defendant with such **Insured Person** solely by reason of such person's status as a spouse or **Common Law Partner**, or such spouse or **Common Law Partner's** ownership interest in property that is sought by a claimant as recovery for an alleged act, error or omission of such **Insured Person**; and

B. the estate, heirs, legal representatives or assigns of such **Insured Person** if such **Insured Person** is deceased or the legal representatives or assigns of such **Insured Person** if such **Insured Person** is incompetent, insolvent or bankrupt.

All terms and conditions of this Policy including, without limitation, the Retention Amount applicable to **Loss** incurred by the **Insured Person**, shall also apply to **Loss** incurred by the **Insured Person's** spouse, **Common Law Partner**, estate, heirs, legal representatives or assigns. The coverage provided by this Section V. shall not apply with respect to any loss arising from an act or omission by an **Insured Person's** estate, heirs, legal representatives, assigns, spouse or **Common Law Partner**.

VI. OTHER INSURANCE

This Policy shall be specifically excess over, and shall not contribute with, any other valid and collectible insurance, whether such other insurance is stated to be primary, contributory, excess (except insurance specifically in excess of this Policy), contingent or otherwise. This Policy will not be subject to the terms of any other insurance.

VII. TERRITORY

Coverage shall extend anywhere in the world.

VIII. EXTENDED REPORTING PERIOD

A. Solely with respect to Insuring Clause A, if the Company or the **Parent Organization** terminates or does not renew this Policy, other than termination by the Company for non-payment of premium, then the **Parent Organization** shall have the right to purchase an Extended Reporting Period for the period set forth in Item 6.(B) of the Declarations beginning on the effective date of the termination or non-renewal of this Policy. This right to purchase an Extended Reporting Period shall lapse unless written notice of election to purchase the Extended Reporting Period, together with payment of the additional premium due, as set forth in Item 6.(A) of the Declarations, is received by the Company within thirty (30) days following the effective date of the termination or non-renewal of this Policy.

B. If the Extended Reporting Period is purchased, then coverage otherwise afforded by this Policy will be extended to apply to **Claims** first made during such Extended Reporting Period and reported in accordance with Section XI. Reporting, but only for **Injury** occurring or allegedly occurring before the effective date of termination or non-renewal or the date of any event described in Section XVI. Changes in Exposure, whichever is earlier. The entire additional premium for the Extended Reporting Period shall be deemed fully earned at the inception of such Extended Reporting Period. Any **Claim** made during the

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 39

Extended Reporting Period shall be deemed to have been made during the immediately preceding **Policy Period**. The Limit of Liability for the Extended Reporting Period shall be part of and not in addition to the applicable Limits of Liability for the immediately preceding **Policy Period**.

IX. LIMIT OF LIABILITY

A. The Company's maximum aggregate liability for all **Loss** and **Expense** covered under this Policy, whether covered under one or more Insuring Clauses, shall be the Aggregate Limit of Liability for each **Policy Period** set forth in Item 3 of the Declarations.

B. The Company's maximum liability for all **Loss** on account of each **Claim** made during the **Policy Period**, or for each **Single Expense** discovered during the **Policy Period**, shall be the applicable Limit of Liability set forth in Item 4 of the Declarations or the unpaid portion of the Aggregate Limit of Liability for each **Policy Period**, whichever is less. If a **Single Expense** is covered under more than one Insuring Clause, the maximum amount payable shall not exceed the largest applicable Limit of Liability.

C. **Defence Costs** are part of and not in addition to the Limits of Liability set forth in Item 4 of the Declarations, and payment by the Company of **Defence Costs** shall reduce and may exhaust such Limits of Liability.

D. Upon exhaustion of the Aggregate Limit of Liability for each **Policy Period** set forth in Item 3 of the Declarations:

1. the Company shall have no further liability for **Loss** or **Expense** regardless of when a **Claim** is made or an **Expense** is discovered, and

2. the Company shall have no obligation to continue the defence of any **Insured** and the **Insureds** shall assume all responsibility for their defence at their own cost.

X. RETENTION AMOUNT AND COINSURANCE

The Company's liability under this Policy shall apply only to that part of each covered **Claim** or **Expense** which is in excess of the applicable Retention Amount set forth in Item 4 of the Declarations. Such Retention Amount shall be depleted only by **Loss** or **Expense** otherwise covered under this Policy and shall be borne by the **Insureds** uninsured and at their own risk.

If different parts of a **Single Expense** are subject to different Retention Amounts, or if a **Claim** and a **Single Expense** arise from any one or a series of related facts, circumstances, situations, transactions, or events, the applicable Retention Amounts will be applied separately to each part of such **Claim** or **Single Expense**, but the sum of such Retention Amounts shall not exceed the largest applicable Retention Amount.

To the extent that **Loss** on account of a single **Claim** or a **Single Expense** is covered under this Policy and is in excess of the Retention Amount, the **Insureds** shall bear uninsured and at their own risk that percentage of such **Loss** or **Expense** specified as the Coinsurance Percentage set forth in Item 5 of the Declarations. The Company's liability shall apply only to the remaining percentage of such **Loss** or **Expense**.

XI. REPORTING

A. With respect to Insuring Clause A:

1. the **Insureds** shall, as a condition precedent to exercising any right to coverage under this Policy, give to the Company written notice of such **Claim** as soon as practicable, but in no event later than the earliest of the following dates:

a. sixty (60) days after the date on which an **Insured Organization's** chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing positions first becomes aware that the **Claim** has been made;

b. sixty (60) days after the effective date of expiration or termination, if this Policy expires (or is otherwise terminated) without being renewed and if no Extended Reporting Period is purchased; or

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 40

© 2015, CCH Canadian Limited

c. the expiration date of the Extended Reporting Period, if purchased;

provided that if the Company sends written notice to an **Insured**, at any time before the date set forth in paragraph A.1.a. of this Section XI, with respect to any **Claim**, stating that this Policy is being terminated for non-payment of premium, the **Insureds** shall give to the Company written notice of such **Claim** prior to the effective date of such termination.

2. If during the **Policy Period** an **Insured** becomes aware of any circumstances which may subsequently give rise to a **Claim**, and during the **Policy Period** the **Insureds**:

   a. give to the Company written notice of such circumstances, including a description of the circumstances in question, the identities of the potential claimants, the consequences which have resulted or may result from the circumstances, the damages which may result from the circumstances and the way in which the **Insureds** first became aware of the circumstances; and

   b. request coverage under this Policy for any **Claim** subsequently arising from such circumstances,

   then the Company will treat any such subsequent **Claim** as if it had been made against an **Insured** during the **Policy Period**; provided that written notice of such **Claim** is then given to the Company in accordance with paragraph A.1.a. of this Section XI.

3. The **Insureds** shall, as a condition precedent to exercising any right to coverage under this Policy, give to the Company such information, assistance and cooperation as the Company may reasonably require, and shall include in any notice under paragraphs A.1. or A.2. of this Section XI, a description of the **Claim** or circumstances, the nature of any alleged **Injury**, the nature of the alleged or potential damage, the names of all actual or potential claimants, the names of all actual or potential parties, and the manner in which an **Insured** first became aware of the **Claim** or circumstances.

B. With respect to Insuring Clauses B through H:

1. The **Insureds** shall, as a condition precedent to exercising any right to coverage under this Policy, give to the Company written notice of any **Expense** as soon as practicable, but in no event later than sixty (60) days after discovery of an **Expense** by an **Insured Organization's** chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing positions.

2. The **Insureds** shall furnish to the Company proof of loss, duly sworn to, with full particulars, within six (6) months after discovery pursuant to paragraph B.1. above.

3. Legal proceedings for the recovery of any **Expense** under this Policy shall not be brought prior to the expiration of sixty (60) days after the proof of loss is filed with the Company or after the expiration of twenty-four (24) months from the discovery of such **Expense**.

4. This Policy affords coverage only in favour of the **Insureds** where legally permissible. No claim, suit, action or legal proceeding shall be brought with respect to Insuring Clauses B through H by anyone other than the **Insureds**.

C. All **Related Claims** shall be treated as a single **Claim** first made on the date the earliest of such **Related Claims** was first made, or on the date the earliest of such **Related Claims** is treated as having been made in accordance with this Section XI, regardless of whether such date is before or during the **Policy Period**.

XII. NOTICE

A. All notices to the Company of **Loss**, **Claims**, **Expense**, or circumstances shall be given in writing addressed to:

Attn: Claims Department

Chubb Insurance Company of Canada

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 41

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®

1 Adelaide Street East

Toronto, ON M5C 2V9

B. All other notices to the Company under this Policy shall be given in writing addressed to:

Attn: Chubb Specialty Insurance - Underwriting

Chubb Insurance Company of Canada

1 Adelaide Street East

Toronto, ON M5C 2V9

C. Any notice given under subsection A. or B. above of this Section XII, shall be effective on the date of receipt by the Company at such address.

XIII. DISCOVERY

With respect to Insuring Clause B, discovery occurs at the earlier of an **Insured Organization's** chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing positions becoming aware of:

A. circumstances which could give rise to an **Expense** of a type covered by this Policy, or

B. an actual or potential claim in which it is alleged that an **Insured** is liable to a third party,

regardless of when the act or acts causing or contributing to such **Expense** occurred, even though the amount of such **Expense** does not exceed the applicable Retention Amount, or the exact amount or details of such **Expense** may not then be known.

With respect to Insuring Clauses E and F, this Policy applies only to loss of a type covered by this Policy first discovered by an **Insured Organization's** chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing positions during the **Policy Period**. Discovery occurs at the earlier of such person being aware of:

A. circumstances which could give rise to a loss of a type covered by this Policy, or

B. an actual or potential claim in which it is alleged that an **Insured** is liable to a third party,

regardless of when the act or acts causing or contributing to such loss occurred, even though the amount of loss does not exceed the applicable Retention Amount, or the exact amount or details of the loss may not then be known.

With respect to Insuring Clause G, this Policy does not cover any **Expense** arising from any **Threat** unless such **Threat** occurs or is communicated directly or indirectly to an **Insured** prior to the effective date of termination of coverage hereunder and is discovered by an **Insured** and communicated to the Company in writing prior to sixty (60) days after the effective date of the termination of this Policy in its entirety.

XIV. DEFENCE AND SETTLEMENT

A. It shall be the duty of the **Insureds** and not the duty of the Company to defend **Claims** made against an **Insured** and to retain qualified counsel of its own choosing with the Company's prior consent, which the Company shall not unreasonably withhold.

B. With respect to any **Claim** that appears reasonably likely to be covered in whole or in part under this Policy, the Company shall have the right and shall be given the opportunity to effectively associate with the **Insureds**, and shall be consulted in advance by the **Insureds** regarding the investigation, defence and settlement of such **Claim**, including but not limited to selecting appropriate defence counsel and negotiating any settlement. It shall not be unreasonable for the Company to withhold its consent to separate counsel for one or more of such **Insureds**, unless there is a material actual or potential conflict of interest among such **Insureds**.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 42

© 2015, CCH Canadian Limited

C. No **Insured** shall settle or offer to settle any **Claim**, incur any **Defence Costs**, or otherwise assume any contractual obligation or admit any liability with respect to any **Claim** without the Company's prior written consent, which the Company shall not unreasonably withhold. The Company shall not be liable for any settlement, **Defence Costs**, assumed obligation or admission to which it has not given its prior written consent.

D. If any **Insured** withholds consent to any settlement acceptable to the claimant in accordance with the Company's recommendation (a "Proposed Settlement"), then the Company's liability for all **Loss**, including **Defence Costs**, from such **Claim** shall not exceed the amount of the Proposed Settlement plus **Defence Costs** incurred up to the date of such **Insured's** refusal to consent to the Proposed Settlement of such **Claim**.

E. The **Insureds** agree to provide the Company with all information, assistance and cooperation which the Company may reasonably require and agree that they will do nothing that may prejudice the Company's position or its potential or actual rights of recovery.

F. The Company shall, upon written request, advance on a current basis **Defence Costs** owed under this Policy. As a condition of any payment of **Defence Costs** before the final disposition of a **Claim**, the Company may require a written undertaking of terms and conditions satisfactory to it guaranteeing the repayment of any **Defence Costs** paid on behalf of any **Insured** if it is finally determined that this Policy would not cover **Loss** incurred by such **Insured** in connection with such **Claim**.

XV. ALLOCATION

A. If both **Loss** covered by this Policy and loss not covered by this Policy are incurred either because a **Claim** against an **Insured** includes both covered and non-covered matters or because a **Claim** is made against both an **Insured** and others, the **Insureds** and the Company shall allocate such amount between covered **Loss** and non-covered loss based upon the relative legal and financial exposures of the parties to covered and non-covered matters and, in the event of a settlement of such **Claim**, also based upon the relative benefits to the parties from such settlement. The Company shall not be liable under this Policy for the portion of such amount allocated to non-covered loss.

B. If the **Insureds** and the Company agree on an allocation of **Defence Costs**, then the Company shall advance on a current basis **Defence Costs** allocated to the covered **Loss**. If the **Insureds** and the Company cannot agree on an allocation:

1. no presumption as to allocation shall exist in any arbitration, suit or other proceeding;

2. the Company shall advance on a current basis **Defence Costs** which the Company believes to be covered under this Policy until a different allocation is negotiated, arbitrated or judicially determined; and

3. the Company, if requested by the **Insureds**, shall submit the dispute to binding arbitration. The rules of the American Arbitration Association shall apply except with respect to the selection of the arbitration panel, which shall consist of one arbitrator selected by the **Insureds**, one arbitrator selected by the Company, and a third independent arbitrator selected by the first two arbitrators.

C. Any negotiated, arbitrated or judicially determined allocation of **Defence Costs** on account of a **Claim** shall be applied retroactively to all **Defence Costs** on account of such **Claim**, notwithstanding any prior advancement to the contrary. Any allocation of advancement of **Defence Costs** 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**.

XVI. CHANGES IN EXPOSURE

A. Acquisition of Another Organization

1. If any **Insured Organization** acquires another entity or merges with another entity (each an "Acquired Organization") such that the **Insured Organization** is the surviving entity, and if as a result of such acquisition or merger the Acquired Organization becomes (or would, but for its absorption into such **Insured Organization**, have become) a **Subsidiary**, then, subject to the

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 43

provisions of paragraphs 2. and 3. below, coverage shall be provided for such Acquired Organization and its **Insured Persons**, with respect to any **Injury** first caused, or **Loss** or **Expense** first incurred, after the effective date of such acquisition or merger. With respect to Insuring Clauses B through H, coverage applies to such Acquired Organization and its **Insured Persons** only for an **Expense** where all of the circumstances, conditions or acts causing or contributing to such **Expense** occur on or after the date of such acquisition or creation.

2. If, at the time of an acquisition or merger described in paragraph 1. above, the annual revenues of the Acquired Organization are equal to or less than ten percent (10%) of the annual revenues of the **Parent Organization**, as reflected in the **Parent Organization's** then most recently concluded fiscal year end financial statements or fiscal quarterly financial statements, then the **Parent Organization** shall provide to the Company written notice of the acquisition or merger containing full details thereof when it next applies for renewal of this Policy. As a condition precedent to providing coverage for such Acquired Organization upon renewal, the Company, in its sole discretion, may impose additional or different terms, conditions and limitations of coverage and require payment of additional premium.

3. If, at the time of an acquisition or merger described in paragraph 1. above, the annual revenues of the Acquired Organization exceed ten percent (10%) of the annual revenues of the **Parent Organization**, as reflected in the **Parent Organization's** then most recently concluded fiscal year end financial statements or fiscal quarterly financial statements, then the **Parent Organization** shall provide to the Company written notice of the acquisition or merger containing full details thereof, as soon as practicable, but in no event later than sixty (60) days after the date of such acquisition or merger. If the **Parent Organization** fails to give such notice within the time specified in the preceding sentence, or fails to pay the additional premium required by the Company, coverage for such Acquired Organization and its **Insured Persons** shall terminate with respect to **Claims** first made or **Loss** or **Expense** first incurred more than sixty (60) days after such acquisition or merger. As a condition precedent to providing coverage for such Acquired Organization or its **Insured Persons**, the Company, in its sole discretion, may impose additional or different terms, conditions and limitations of coverage and require payment of additional premium.

B. Cessation of Subsidiaries

If any **Subsidiary** ceases to be a **Subsidiary** before or during the **Policy Period**, then any coverage under this Policy shall continue for such **Subsidiary** and its **Insured Persons** until the expiration of this Policy, but solely for **Injury** first caused, or **Loss** or **Expense** first incurred, prior to the effective date of such cessation and on or after the **Retroactive Date** shown in Item 7 of the Declarations.

C. Conversion of Coverage Under Certain Circumstances

If, during the **Policy Period**, any of the following events occur:

1. the acquisition of all, or substantially all of the **Parent Organization's** assets by another organization or natural person or group of organizations and/or natural persons acting in concert, or the merger or consolidation of the **Parent Organization** into or with another entity such that the **Parent Organization** is not the surviving entity;

2. another organization, natural person or group of organizations and/or natural persons acting in concert acquires securities or voting rights which results in ownership or voting control by the other organization(s) or natural person(s) of more than fifty percent (50%) of the outstanding securities representing the present right to vote for the election of directors, trustees, members of the Board of Managers or management committee members of the **Parent Organization**;

3. the **Parent Organization** completely ceases to actively engage in its primary business ("cessation"); or

4. **Financial Impairment**,

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 44

© 2015, CCH Canadian Limited

then coverage provided by this Policy shall continue until its expiration, but solely for **Injury** first caused, or **Loss** or **Expense** first incurred, prior to such event and on or after the **Retroactive Date** shown in Item 7 of the Declarations.

The **Parent Organization** shall give written notice of such event to the Company as soon as practicable together with such other information as the Company may request, and the entire premium for this Policy will be deemed fully earned as of the date of such event.

XVII. REPRESENTATIONS AND SEVERABILITY

In issuing this Policy, the Company has relied upon the statements, representations and information in the **Application**. All of the **Insureds** acknowledge and agree that all such statements, representations and information (i) are true and accurate, (ii) were made or provided in order to induce the Company to issue this Policy, and (iii) are material to the Company's acceptance of the risk to which this Policy applies.

In the event that any of the statements, representations or information in the **Application** are not true and accurate, this Policy shall be void with respect to any **Insured** who knew as of the effective date of the **Application** the facts that were not truthfully and accurately disclosed (whether or not such **Insured** knew of such untruthful disclosure in the **Application**) or to whom knowledge of such facts is imputed.

For purposes of the preceding sentence:

A. the knowledge of any **Insured Person** who is a past, present or future chief financial officer, in-house general counsel, risk manager, president, chief executive officer, chief information officer, chairperson or equivalent position of any of the foregoing positions of an **Insured Organization** shall be imputed to such **Insured Organization**;

B. the knowledge of the person(s) who signed the **Application** for this Policy shall be imputed to all of the **Insureds**; and

C. except as provided in A. above, the knowledge of an **Insured Person** who did not sign the **Application** shall not be imputed to any other **Insured**.

XVIII. VALUATION AND FOREIGN CURRENCY

Unless otherwise designated in the Declarations, all premiums, limits, Retention Amounts, **Loss, Expense** and other amounts under this Policy are expressed and payable in the currency of Canada. If a judgment is rendered, a settlement is denominated or any element of **Loss** or **Expense** under this Policy is stated in a currency other than Canadian dollars, payment under this Policy shall be made in Canadian dollars at the rate of exchange published in The Globe and Mail on the date the final judgement is reached, the amount of the settlement is agreed upon or the element of **Loss** or **Expense** is due, respectively.

With respect to Insuring Clauses D through H, the value of any loss of property other than **Data** or **Media** shall be the actual cash value or the cost of repairing or replacing such property with property of like quality and value, whichever is less.

XIX. SUBROGATION

In the event of any payment under this Policy, the Company shall be subrogated to the extent of such payment to all the **Insureds'** rights of recovery therefore, and the **Insureds** shall execute all papers required and shall do everything necessary to secure and preserve such rights, including the execution of such documents necessary to enable the Company effectively to bring suit or otherwise pursue subrogation rights in the name of any **Insured**.

XX. ACTION AGAINST THE COMPANY

No action may be taken against the Company unless, as a condition precedent thereto, there shall have been full compliance with all the terms of this Policy. No person or entity shall have any right under this Policy to join the Company as a party to any action against any **Insured** to determine such **Insured's** liability nor shall the Company be impleaded by such **Insured** or legal representatives of such **Insured**.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 45

XXI. PARENT ORGANIZATION RIGHTS AND OBLIGATIONS

By acceptance of this Policy, the **Parent Organization** acknowledges and agrees that it shall be considered the sole agent of and will act on behalf of each **Insured** with respect to: the payment of premiums and the receiving of any return premiums that may become due under this Policy; the negotiation, agreement to and acceptance of endorsements; the giving or receiving of any notice, including but not limited to giving notice of **Claim**, **Loss** or **Expense,** a notice of termination pursuant to Section XXIII. Termination of Policy; and the receipt or enforcement of payment of a **Loss** (and the **Parent Organization** shall be responsible for application of any such payment as provided for in this Policy). Each **Insured** acknowledges and agrees that the **Parent Organization** shall act on its behalf with respect to all such matters.

XXII. ALTERATION AND ASSIGNMENT

No change in, modification of, or assignment of interest under this Policy shall be effective except when made by a written endorsement to this Policy which is signed by an authorized employee of Chubb Insurance Company of Canada.

XXIII. TERMINATION OF POLICY

A. This Policy shall terminate at the earliest of the following times:

1. sixty (60) days after receipt by the **Parent Organization** of written notice of non-renewal from the Company;

2. upon receipt by the Company of written notice of termination from the **Parent Organization**; provided that this Policy may not be terminated by the **Parent Organization** after the effective date of any event described in Subsection C. of Section XVI, Changes in Exposure;

3. upon expiration of the **Policy Period** as set forth in Item 2 of the Declarations;

4. twenty (20) days after receipt by the **Parent Organization** of a written notice of termination from the Company based upon non-payment of premium, unless the premium is paid within such twenty (20) day period; or

5. at such other time as may be agreed upon by the Company and the **Parent Organization**.

B. The Company shall refund the unearned premium computed at customary short rates if this Policy is terminated by the **Parent Organization**. Under any other circumstances the refund shall be computed pro rata. Payment or tender of any unearned premium by the Company shall not be a condition precedent to the effectiveness of such termination, but such payment shall be made as soon as practicable.

XXIV. BANKRUPTCY

Except as provided in Section XVI. Changes in Exposure, bankruptcy or insolvency of any **Insured** shall not relieve the Company of its obligations nor deprive the Company of its rights or defences under this Policy.

XXV. COMPLIANCE WITH APPLICABLE TRADE SANCTION LAWS

This insurance does not apply to the extent that trade or economic sanctions or other laws or regulations prohibit the Company from providing insurance.

XXVI. HEADINGS

The descriptions in the headings and sub-headings of this Policy are solely for convenience, and form no part of the terms and conditions of coverage.

XXVII. **SINGULAR OR PLURAL**

Terms used in this Policy in the singular have the same meaning where used in the plural.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 46

© 2015, CCH Canadian Limited

¶43-746b Sample Privacy Policy Application

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

BY COMPLETING THIS APPLICATION YOU ARE APPLYING FOR COVERAGE WITH CHUBB INSURANCE COMPANY OF CANADA (THE "COMPANY")

NOTICE: INSURING CLAUSE "A" OF THE CYBERSECURITY BY CHUBB® POLICY PROVIDES CLAIMS MADE COVERAGE, WHICH APPLIES ONLY TO "CLAIMS" FIRST MADE DURING THE "POLICY PERIOD," OR ANY APPLICABLE EXTENDED REPORTING PERIOD. INSURING CLAUSES "B" THROUGH "H" OF THE CYBERSECURITY BY CHUBB® POLICY PROVIDE FIRST PARTY COVERAGE. EXCEPT WHEN PROHIBITED BY THE LAWS OF THE PROVINCE OF QUEBEC, THE LIMIT OF LIABILITY TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY "DEFENCE COSTS". "DEFENCE COSTS" WILL BE APPLIED AGAINST THE RETENTION. IN NO EVENT, OTHER THAN WHEN PROHIBITED BY THE LAWS OF THE PROVINCE OF QUEBEC, WILL THE COMPANY BE LIABLE FOR "DEFENCE COSTS" OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF LIABILITY. THE COVERAGE AFFORDED UNDER THIS POLICY DIFFERS IN SOME RESPECTS FROM THAT AFFORDED UNDER OTHER POLICIES. READ THE ENTIRE APPLICATION CAREFULLY BEFORE SIGNING.

APPLICATION INSTRUCTIONS:

1. Whenever used in this Application, unless otherwise stated, the term "**Applicant**" means the Parent Organization and all of its Subsidiaries.
2. Please include all requested underwriting information and attachments and provide a complete response to all questions and attach additional pages if necessary
3. Please sign and date this CyberSecurity New Business Application

I.	**GENERAL APPLICANT INFORMATION (FOR ALL APPLICANTS)**					
1.	Name of the **Applicant**:					
2.	Address of the **Applicant** (including Postal Code):					
	Telephone Number:					
3.	Website Address(es):					
4A.	Name and Title of Primary Contact					
4B.	Address and Telephone Number of Primary Contact if different from Question 2					
5.	The **Applicant** is:	☐ Individual	☐ Non-Profit	☐ Partnership	☐ Privately Held Corporation	
		☐ Publicly Traded Corporation	☐ Other (describe)			
6.	Year **Applicant** was established					
7.	Are there affiliates or other related entity(ies) (including "Doing Business As" entities) for which coverage is desired? If Yes, list all such entities on a separate sheet and attach it to this Application.				☐ Yes	☐ No
NOTE: Coverage is not afforded to any such affiliate or related entity (other than a Subsidiary) unless it is scheduled in this section of the Application and specifically named as an Insured on the policy.						
8.	Describe the Applicant's Principal Operations:					

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 47

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

II.	**QUANTIFIABLE INFORMATION**				
1.	The following should be, for each category, the sum of the applicable information for the Parent Organization plus the applicable information for all Subsidiaries applying for this insurance.				
	Item	**Last Fiscal Year**	**This Fiscal Year**	**Projected for Next Fiscal Year**	
A.	Number of Employees				
B.	Number of Online Customers				
C.	Total Number of owned or dedicated servers				
D.	Total Number of Active IP Addresses				
E.	Consolidated Total Assets	$	$	$	
F.	Consolidated Gross Revenues	$	$	$	
G.	Consolidated Gross Revenues from Online Sales or Services	$	$	$	
2.	**Coverage and Limits of Liability Requested**				
	Insuring Clause	**Limit of Liability**	**Retention Amount**		
	Mandatory Coverage				
	A. CyberLiability (includes: Conduit, Content, Disclosure, Impaired Access, and Reputational Injury)	$	$		
	Optional Coverage (Please tick the box for each Coverage the **Applicant** seeks)				
☐	B. Privacy Notification Expenses	$	$		
☐	C1. Crisis Management Expenses	$	$		
☐	C2. Reward Expenses	$	$		
☐	D. E-Business Interruption and Extra Expenses	$	$		
☐	E. E-Theft Loss	$	$		
☐	F. E-Communication Loss	$	$		
☐	G. E-Threat Expenses	$	$		
☐	H E-Vandalism Expenses	$	$		
3.	Policy Period Requested	From:	To:		
4.	In the next twelve (12) months, does the **Applicant** anticipate establishing or entering into any related or unrelated ventures which are a material change in operations? If yes, please describe:			☐ Yes	☐ No

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 48

© 2015, CCH Canadian Limited

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

A. Information Systems Security Policy			
1.	Does the **Applicant's** information security policy identify and stipulate the types and levels of protection for all of the **Applicant's** information assets, whether electronic or otherwise, and whether held by the **Applicant** or by a person or organization providing services to the **Applicant**? If No, please explain why:	☐ Yes	☐ No
2.	Does the **Applicant** test the security levels required by the security policy at least annually?	☐ Yes	☐ No
3.	Does the **Applicant** regularly identify and assess new threats and adjust the security policy to address such new threats?	☐ Yes	☐ No
4.	Does the **Applicant** collect, store or process personally identifiable or other confidential information? If yes, please describe the nature of the prospective, current and former Customer and employee records held (including employee records) and comment on the **Applicant's** record retention policy, indicating the length of time such records are kept (either active or in archives) and how they are stored.	☐ Yes	☐ No
5.	Does the **Applicant** store sensitive data on its Web servers?	☐ Yes	☐ No
6.	Does the **Applicant** shred all written or printed personally identifiable or other confidential information when it is being discarded?	☐ Yes	☐ No
7.	Does the **Applicant** process or store personally identifiable or other confidential information for or on behalf of third parties? If Yes, please describe:	☐ Yes	☐ No
B. Laptop / Mobile Device Security Policy			
1.	Does the **Applicant** have a laptop security and/or mobile device policy?	☐ Yes	☐ No
2.	Does the **Applicant** encrypt data held on laptops and/or mobile devices?	☐ Yes	☐ No
3.	In the past 24 months how many laptops or mobile devices have been lost or stolen?		
4.	Please describe the **Applicant's** protocols when a laptop or mobile device is discovered to be missing.		
C. Third Party Electronic Service Providers:			
1.	Does the **Applicant** use third party electronic service providers? If Yes, please indicate which types of third party service providers are used	☐ Yes	☐ No
	☐ Website ☐ Applications (ASP) ☐ Infrastructure ☐ Operations ☐ Back up / Archiving		

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 49

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

	☐ Other – Please describe		
2.	Is a written agreement in place between the **Applicant** and third party providers?	☐ Yes	☐ No
3.	Does the agreement require a level of security commensurate with the **Applicant's** information systems security policy?	☐ Yes	☐ No
4.	Does the **Applicant** review the results of each service provider's most recent SAS 70 or commensurate risk assessment?	☐ Yes	☐ No
5.	Does the agreement state that the service provider has primary responsibility for the security of the **Applicant's** information?	☐ Yes	☐ No
6.	Does the agreement include contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data?	☐ Yes	☐ No
7.	How frequently does the **Applicant** back up electronic data?		
8.	Please provide any comments in respect of the **Applicant's** use of third party service providers or contracting practices that the **Applicant** wishes to amplify:		
D. Disaster Recovery (DRP) and Business Continuity Plans (BCP)			
1.	Does the **Applicant** have a computer DRP and/or BCP?	☐ Yes	☐ No
2.	Are the DRP and/or BCP reviewed and updated at least bi-annually?	☐ Yes	☐ No
3.	Are the DRP and/or BCP recovery plan tested at least annually?	☐ Yes	☐ No
4.	Is the DRP and/or BCP reviewed and approved by the **Applicant's** Board of Directors (or persons with substantially similar responsibilities) at least bi-annually?	☐ Yes	☐ No
E. Incident Response Plans (IRP)			
1.	Does the **Applicant** have a formal, written IRP that addresses:		
1A.	Unauthorized access to the **Applicant's** computers, system, network or any of the **Applicant's** information assets?	☐ Yes	☐ No
1B.	Denial of service attacks and other forms of network or system outages?	☐ Yes	☐ No
1C.	Extortion demands?	☐ Yes	☐ No
1D.	Corruption of, or damage to, data?	☐ Yes	☐ No
2.	Does the IRP include a review by the **Applicant's** legal counsel of any provincial, territorial, state or federal laws or regulations that may affect the **Applicant's** response or other standards with which the **Applicant** may have to comply?	☐ Yes	☐ No
3.	Does the **Applicant** conduct a full test of the IRP at least annually and address or correct any issues or problems identified in the tests?	☐ Yes	☐ No
4.	Has the **Applicant** estimated the financial cost to respond to an incident of unauthorized access to personally identifiable or other — Estimated Cost $	☐ Yes	☐ No

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 50

© 2015, CCH Canadian Limited

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

	confidential information (i.e. data breach)? If Yes, what is the estimated cost?			
5.	Does the IRP identify the organization that will provide:			
5A	Legal advice?		☐ Yes	☐ No
5B	Mailing or other notification services?		☐ Yes	☐ No
5C	Public relations services?		☐ Yes	☐ No
5D	Credit or other monitoring services?		☐ Yes	☐ No
5E	Forensic services?		☐ Yes	☐ No
F. Vulnerability or Penetration Testing, Virus Prevention and Intrusion Detection				
1.	Does the **Applicant** run vulnerability or penetration testing against all parts of its network? If Yes, how frequently are the tests run?	Frequency of Testing	☐ Yes	☐ No
2.	Are anti-virus programs installed on all of the **Applicant's** PCs, Laptops and network systems? If yes, how frequently are the detections systems updated?	Frequency of Updating	☐ Yes	☐ No
3.	Does the **Applicant** employ intrusion detection or intrusion protection devices on its network, IDS or IPS software on the **Applicant's** hosts? If Yes, how frequently are logs reviewed?	Frequency of Log Review	☐ Yes	☐ No
G. Security Assessments				
1.	Has an external systems security assessment, other than vulnerability scans or penetration tests been conducted in the past 12 months? If Yes, please indicate who conducted the assessment, attach a copy of the results; and indicate whether all critical observations or recommendations have been complied with. If No, please explain why.		☐ Yes	☐ No
H. Legal Compliance				
1.	Due to the **Applicant's** operations, is it specifically subject to any federal, provincial, territorial, or state law or regulation concerning privacy or the safeguarding of personally identifiable or other confidential information? If Yes, please describe the specific laws, regulations or SRO guidelines that apply to the **Applicant's** operations (for example, in Canada: PIPEDA, PIPA, HIPA, PHIA, PHIPA, QPPIPS, the Bank Act, etc or in the US: HIPPA, Gramm, Leach Billey Act or any other similar laws in other jurisdictions)		☐ Yes	☐ No

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 51

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

III.	**PAYMENT CARD INDUSTRY COMPLIANCE (PCI)** – please answer the following questions if the **Applicant** is subject to PCI Security Standards		☐ N/A
1.	How many credit or debit card transactions does the **Applicant** process annually?		
2.	Does the **Applicant**:		
2A.	Mask all but the last four digits of a card number when displaying or printing cardholder data?	☐ Yes	☐ No
2B.	Ensure that card-validation codes are not stored in any of the **Applicant's** databases, log files or anywhere else in its network?	☐ Yes	☐ No
2C.	Encrypt all account information on the **Appilcant's** databases?	☐ Yes	☐ No
2D.	Encrypt of use tokenization for all account information at the point of sale?	☐ Yes	☐ No
IV.	**SECURITY INCIDENT AND LOSS HISTORY**		
1.	Has the Applicant had any computer or network security incidents during the past two (2) years? "Incident" includes any unauthorized access or exceeding authorized access to any computer, system, data base or data; intrusion or attack; the denial of use of any computer or system; intentional disruption, corruption or destruction of electronic data, programs or applications; or any other incidents similar to the foregoing? *Note: if the answer to this Question is Yes, please attach a complete description of the incident(s), including whether you reported the incident(s) to law enforcement and/or your insurance carrier.*	☐ Yes	☐ No
2.	If Yes, to Question IV. 1, in the past two years have such incidents:		
	☐ Increased in frequency	☐ Decreased in frequency	☐ Remained unchanged
V.	**ATTACHMENTS AND OTHER DOCUMENTS**		
	Please identify what additional documents are attached to, and/or submitted in conjunction with, this Application. All such documents are considered part of this Application.		
☐	List of all subsidiaries to be covered. *(Note: If a policy is issued, only those organizations listed on this attachment will be Insureds, unless an entity is subject to the Newly Acquired or Formed Organization condition.)*		
☐	A description of any security incident or Loss, as requested in Section III. Question 1 or Section IV. Question 1.		
☐	CyberSecurity By Chubb® Risk Matrix, if requested by a Chubb Underwriter		
☐	Supplementary Questionnaires, if applying for more than $5,000,000 in Limits of Liability		
☐	Application from another insurance company for coverage that is similar to CyberSecurity By Chubb®		
☐	Risk assessment of the **Applicant** that has been performed by an organization other than the **Applicant**		
☐	Other information or additional explanations that the **Applicant** wishes to include in support of this Application		
VI.	**REPRESENTATION: PRIOR KNOWLEDGE OF FACTS/CIRCUMSTANCES/SITUATIONS:**		
1.	No person who would be an Insured Person under the proposed coverage is aware of any fact, circumstance, or situation which he or she has reason to suppose might give rise to any claim that would fall within the scope of the proposed coverage, except: (If necessary, attach a full description to answer this warranty question)	☐ None or explain:	

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 52

© 2015, CCH Canadian Limited

Chubb Insurance Company of Canada
1 Adelaide Street East, Toronto, ON M5C 2V9

CYBERSECURITY BY CHUBB®
***New Business* Application**

Without prejudice to any other rights and remedies of the Company, the signer(s) of this Application**,** on his or her own behalf and on behalf of any organization or person that would qualify as an Insured under the proposed coverage, understands and agrees that if any such fact, circumstance, or situation exists, whether or not disclosed above in response to this Question VI 1., then any claim or action arising from such fact, circumstance, or situation is excluded from coverage under the proposed policy, if issued by the Company.	
VII.	**MATERIAL CHANGE**
If there is any material change in the answers to the questions in this Application before the policy inception date, the **Applicants** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.	
VIII.	**DECLARATIONS, FRAUD WARNINGS AND SIGNATURES**
The **Applicant's** submission of this Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this Application. The undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this Application and any attachments or information submitted with this Application, are true and complete. The undersigned agree that this Application and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued. The Company will have relied upon this Application, its attachments, and such other information submitted therewith in issuing such policy. The information provided in this Application is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.	
This Application must be signed by the chief executive officer and chief financial officer of the Parent Organization acting as the authorized representatives of the person(s) proposed for this insurance.	

Date:	Signature of Applicant:	Title
		☐ Chief Executive Officer; or ☐ Chief Financial Officer (Mark the title that applies)

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 53

¶43-770 CASE LAW/LEGISLATION

¶43-772 Case Law

Jones v. Tsige[68]

In 2012, the Ontario Court of Appeal recognized the new common law tort of intrusion upon seclusion in the landmark decision of *Jones v. Tsige*. The Court awarded $10,000 in damages to a man whose former wife, a bank employee, had, 174 times, inappropriately accessed personal banking information relating to her ex-husband's new partner. The Court imposed a cap of $20,000 where there has been no pecuniary loss, and although the possibility exists for punitive or aggravated damages on top of this amount, such damages would only be awarded in exceptional cases.

Landry v. Royal Bank of Canada[69]

In 2011, the Federal Court ordered a Canadian bank to pay damages in respect of a breach of the federal privacy legislation by one of its employees. Contrary to the bank's policies, the employee had, in response to a subpoena, provided private bank information to a customer's ex-spouse who was involved in a contested divorce.

Despite arguments challenging the cause of the complainant's alleged "humiliation" being related to the privacy breach, the Court found that the breach warranted damages in the amount of $4,500, plus interest and costs.

Demcak v. Vo[70]

In May 2013, the Supreme Court of British Columbia held that there is no common law tort of invasion or breach of privacy in British Columbia, contrary to the ruling by the Ontario Court of Appeal in *Jones v. Tsige* (see discussion above).

This case dealt with an alleged trespass by the City of Richmond and the property management company acting on behalf of the owner of a property which was being sublet by the plaintiffs. The plaintiffs alleged that the City and the property management company "insisted or forced themselves" into vehicles owned by the plaintiffs after the plaintiffs failed to remove the vehicles from the property. No actual damages or injury to the vehicles, nor any loss of use of the vehicles, was mentioned in the pleading. In addition to finding that there is no common law tort of privacy in British Columbia, the Court further ruled that the inspections carried out by the City and the property management company fell outside the tort creation by section 1 of the BC *Privacy Act*.

[68] 2012 ONCA 32.
[69] 2011 FC 687.
[70] 2013 BCSC 899

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 54

© 2015, CCH Canadian Limited

¶43-774 Legislation

Application of privacy legislation across Canada is as follows:

Jurisdiction	Legislation
Federal	• *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 ("PIPEDA")[71] • *Privacy Act*, RSC 1985, c. P-21
Alberta	• *Personal Information Protection Act*, SA 2003, c. P-6.5 • *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25 • *Health Information Act*, RSA 2000, c. H-5
British Columbia	• *Personal Information Protection Act*, SBC 2003, c. 63, • *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 • *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c. 38
Manitoba	• PIPEDA, SC 2000, c. 5 • *Freedom of Information and Protection of Privacy Act*, CCSM, c. F175 • *Personal Health Information Act*, CCSM, c. P33.5 • *Personal Information Protection and Identity Theft Prevention Act*, CCSM, c. P33.7
New Brunswick	• PIPEDA, SC 2000, c. 5 • *Right to Information and Protection of Privacy Act*, SNB 2009, c. R-10.6 • *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05
Newfoundland and Labrador	• PIPEDA, SC 2000, c. 5 • *Access to Information and Protection of Privacy Act*, 2002, c. A-1.1 • *Personal Health Information Act*, SNL 2008, c. P-7.01
Nova Scotia	• PIPEDA, SC 2000, c. 5 • *Freedom of Information and Protection of Privacy Act*, SNS 1993, c. 5 • *Personal Health Information Act*, SNS 2010, c. 41[72]
Ontario	• PIPEDA, SC 2000, c. 5 • *Freedom of Information and Protection of Privacy Act*, RSO 1990, c. F.31 • *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c. M.5 • *Personal Health Information Act, 2004*, SO 2004, c. 3, Schedule A
Prince Edward Island	• PIPEDA, SC 2000, c. 5 • *Freedom of Information and Protection of Privacy Act*, c. F-15.01
Quebec	• *An Act respecting the protection of personal information in the private sector*, RSQ, c. P-39.1 • *An Act respecting access to documents held by public bodies and the protection of personal information*, RSQ, c. A-2.1

[71] PIPEDA applies to all federal and provincial cross-border transfer of personal information in a commercial activity.

[72] This Act was proclaimed on December 4, 2012 and came into force on June 1, 2013.

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 55

Saskatchewan	• PIPEDA, SC 2000, c. 5 • *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. F-22.01 • *Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. L-27.1 • *Health Information Protection Act*, SS 1999, c H-0.021
Northwest Territories	• PIPEDA, SC 2000, c. 5 • *Access to Information and Protection of Privacy Act*, SNWT 1994, c. 20
Nunavut	• PIPEDA, SC 2000, c. 5 • *Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c. 20
Yukon	• PIPEDA, SC 2000, c. 5 • *Access to Information and Protection of Privacy Act*, RSY 2002, c. 1

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 56

© 2015, CCH Canadian Limited

¶43-790 FURTHER INFORMATION

¶43-792 Privacy Commissioners by Jurisdiction

Jurisdiction	Commissioner	Website
Federal	Jennifer Stoddart, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada	http://www.priv.gc.ca/au-ans/index_e.asp
Alberta	Jill Clayton, Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of Alberta	http://www.oipc.ab.ca/pages/home/default.aspx
British Columbia	Elizabeth Denham, Information and Privacy Commissioner for British Columbia, Office of the Information & Privacy Commissioner for British Columbia	http://www.oipc.bc.ca/
Manitoba	Mel Holley, Acting Ombudsman for the Province of Manitoba, Office of the Ombudsman	http://www.ombudsman.mb.ca/
New Brunswick	Anne E. Bertrand, Q.C., Access to Information and Privacy Commissioner, Office of the Access to Information and Privacy Commissioner	http://www2.gnb.ca/content/gnb/en/contacts/dept_renderer.201145.html
Newfoundland and Labrador	Ed Ring, Commissioner, Office of the Information and Privacy Commissioner	http://www.oipc.nl.ca/
Nova Scotia	Dulcie McCallum, Review Officer, The Nova Scotia Freedom of Information and Protection of Privacy Review Office	http://www.foipop.ns.ca/
Ontario	Dr. Ann Cavoukian, Commissioner Information and Privacy Commissioner, Ontario	http://www.ipc.on.ca/english/Home-Page/
Prince Edward Island	Maria C. MacDonald, Information and Privacy Commissioner of Prince Edward Island	http://www.assembly.pe.ca/index.php?number=1013943
Quebec	Me Jean Chartier, Président, Commission d'accès à l'information du Québec	http://www.cai.gouv.qc.ca/diffusion-de-linformation/
Saskatchewan	Gary Dickson, Q.C., Information and Privacy Commissioner, Office of the Saskatchewan Information and Privacy Commissioner of Saskatchewan	http://www.oipc.sk.ca/
Northwest Territories	Elaine Keenan Bengts, Information and Privacy Commissioner of the Northwest Territories	N/A
Nunavut	Elaine Keenan Bengts, Information and Privacy Commissioner of Nunavut	http://www.info-privacy.nu.ca/
Yukon	Diane McLeod-McKay, Yukon Ombudsman and Yukon Information & Privacy Commissioner of the Yukon	http://www.ombudsman.yk.ca/

REMOVE Username: Iver.Chong Date: 11-FEB-15 Time: 13:26 Filename: D:\reports\uccg\master\sf14201.dat Seq: 57