CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

The 2020 Ottawa Region
Charity & Not-for-Profit Law
Seminar
February 13, 2020

Navigating Privacy Breaches For Charities & NFPs

By Esther Shainblum B.A., LL.B., LL.M, CRM
eshainblum@carters.ca
1-877-942-0001

OVERVIEW

- What Is Personal Information?
- What Is A Privacy Breach?
- A Snapshot of The Problem
- Possible Consequences of A Privacy Breach
- Boards of Directors and Liability For Privacy Breaches
- PIPEDA Requirements – Breach Prevention
- Reduce The Risk of Privacy Breaches
- Preparing For A Privacy Breach
- Responding To A Privacy Breach
- Legal Privilege For Privacy Breach Investigations
- Other Expert Advisors

3

A. WHAT IS PERSONAL INFORMATION?

- "Any information about an identifiable individual"
- Examples of personal information:
  - Name, address
  - Health card number
  - Financial information
  - Anything that pertains to a person's health care
  - The identity of a person's health care provider
  - Images of identifiable individuals
  - Video surveillance - whether or not recorded

www.charitylaw.ca www.carters.ca

4

B. WHAT IS A PRIVACY BREACH?

- A "privacy breach" is the loss of, unauthorized access to, use or disclosure of personal information
- Common examples include when:
  - Unencrypted portable devices containing personal information are lost or stolen *e.g.*, laptops, USB keys, tablets, external hard drives
  - Personal information is mistakenly faxed or emailed to the wrong person
  - Employees access personal information without authorization (snooping)
  - Documents or devices are improperly disposed of

www.charitylaw.ca www.carters.ca

5

- Privacy breaches can also result from cyber attack incidents such as:
  - Hacking (exploiting weaknesses in a computer system or network)
  - Data theft
  - Ransomware (where hackers use malicious software to block access to a computer system until a ransom is paid)
  - Phishing (pretending to be someone to trick people into giving you sensitive information)
  - Social engineering (tricking people into giving you money or data)

www.charitylaw.ca www.carters.ca

6

C. A SNAPSHOT OF THE PROBLEM

- The Office of the Privacy Commissioner of Canada ("OPC") reported that, between November 1, 2018, when breach reporting under PIPEDA became mandatory, and October 31, 2019, 28 million Canadians were affected by a data breach
- 58% of reported breaches involved unauthorized access:
  - Employee snooping
  - Phishing and impersonation
- 12% of breaches were due to loss of computer, storage drive or paper documents

www.charitylaw.ca www.carters.ca

7

- 8% of the breaches resulted from theft of documents or computer hardware
- 5% of the breaches resulted from accidental disclosure *e.g.* documents emailed or mailed to the wrong person
- And it is not just big businesses
- A 2016 US survey found that 63% of non-profits had a privacy breach that year
- In that survey, more breaches (20%) were caused by lost devices and lost paper files than by hackers (17%) but hacking incidents were found to be much more expensive and disruptive

www.charitylaw.ca www.carters.ca

8

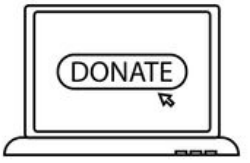
D. POSSIBLE CONSEQUENCES OF A PRIVACY BREACH

- Privacy breaches are a real risk for all organizations
- Can result in:
  - Legal liability, including litigation, possibly class action
  - Regulatory investigations and enforcement
  - Business interruption (*e.g.* ransomware)
  - Financial loss – average cost of a data breach in Canada is $4.4 million US$ (Ponemon Institute Report 2019)
  - Reputational damage – perhaps most important in the charity and NFP sector
- "It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it." – Stephane Nappo (Global Chief Information Security Officer & Board Advisor, Société Générale IBFS)

www.charitylaw.ca www.carters.ca

9

- Majority of Canadians make financial donations to charities or NFPs
- Majority of Canadians prefer to donate online
- In the 2018 Global Trends in Giving Report, 92 percent of donors said it was important for charities to protect their financial and contact information from data breaches
- How can charities and other NFPs maintain the trust and confidence of their donors, clients and other stakeholders, and minimize the risk of reputational damage?



10

- Under the *Canada Not-for-Profit Corporations Act* ("CNCA"), the *Ontario Not-for-Profit Corporations Act* ("ONCA") (expected to be proclaimed in 2020), and *Ontario Corporations Act* ("OCA") directors and officers are required to:
  - act honestly and in good faith with a view to the best interests of the company; and
  - exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances


Reasonable Person

11

- Directors and officers of charities and NFPs impacted by privacy breaches may be exposed to the risk of litigation and claims that they are liable for the breach
- The "Business Judgment Rule" protects directors and senior officers against hindsight and second guessing by third parties and the courts, provided that the directors have made an informed and reasonable decision
- Directors are also entitled to rely in good faith on reports of expert advisors

12

- Directors can show that they met the duty of care and made an informed, reasonable decision by, for example:
  - Demonstrating that they had information available to them and how they considered it
  - Obtaining expert advice on privacy and cybersecurity
  - Confirming that the organization has appropriate safeguards in place to protect personal information
  - Confirming that the organization has appropriate policies and procedures in place, including taking steps to prepare for and respond to breaches
  - Obtaining regular reports from management on cybersecurity and privacy issues
  - Obtaining insurance to cover these risks

13

F. PIPEDA REQUIREMENTS - BREACH PREVENTION

- PIPEDA applies to every organization – including charities and NFPs - in respect of the personal information that it collects, uses or discloses in the course of commercial activities
- Most prudent for charities and NFPs to assume that the OPC or a court might find that they are engaged in commercial activity and that they are subject to PIPEDA
- Charities and NFPs should consider voluntary compliance with PIPEDA, whether required or not
- OPC - Charities and NFPs can benefit from complying with PIPEDA's underlying "fair information principles"

14

- PIPEDA principle 4.7 requires organizations to protect personal information by security safeguards appropriate to the sensitivity of the information
- The security safeguards must protect personal information against loss or theft, unauthorized access, disclosure, copying, use, or modification regardless of the format in which it is held
- The safeguards should include
  - Physical measures, such as:
    - Locking/securing doors, storage cabinets, premises
    - Restricting access to certain areas
    - Access cards and keys

15

- Organizational/administrative measures, such as
  - Security clearances
  - Limiting employee access to personal information on a "need-to-know" basis
  - Privacy and security policies and procedures
  - Implementing and enforcing policies
  - Training
- Technological measures, such as:
  - Passwords and encryption
  - Anti-virus, anti-malware software
  - Firewalls
  - Updating software
  - Cyber security audits

www.charitylaw.ca www.carters.ca

16

G. REDUCE THE RISK OF PRIVACY BREACHES

- Many privacy breach risks can be mitigated by taking some basic steps, such as:
  - Do not collect or retain more personal information than is necessary
  - Encrypt and password protect laptops, USB keys and other portable devices
  - Avoid placing personal information on mobile devices
  - Avoid sending sensitive personal information by email or on wireless networks unless encrypted
  - Avoid faxing personal information as, *e.g.*, it is easily misdirected and could leave personal information publicly exposed
  - Make sure personal information, including hardware, is securely retained and disposed of
  - Use physical safeguards to protect personal information – such as locking office doors, filing cabinets, server rooms

www.charitylaw.ca www.carters.ca

17

- Build a culture of privacy – have ongoing employee privacy and security training to ensure they understand the risks and their responsibilities
- Limit employee access to personal information on a "need to know" basis and put audit trails in place
- Have strong privacy safeguards in your contracts with third parties
- Have appropriate and up-to-date anti-virus and anti-malware software
- Have appropriate systems in place to prevent hacking, intrusions and other threats to your network

18

H. PREPARING FOR A PRIVACY BREACH

- The question is when, not if, a privacy breach will occur
- Organizations should be prepared ahead of time
- As part of that preparation it is important to develop a clear picture of your data practices including:
  - The jurisdiction(s) you operate in
  - What personal information you collect and why
  - How sensitive it is?
  - Where it is stored?
  - Who accesses it?
  - Whether it is transferred to third parties such as service providers

19

- Based on that preliminary work, the organization should put in place an incident response plan
- Having a plan in place will provide guidance for how a privacy breach should be handled if it occurs
- The plan would identify the internal and external personnel who would respond to a privacy breach, set out their roles and responsibilities and outline the procedures for responding to an incident
- Incident response plans should ensure that the organization complies with legal requirements, such as breach reporting obligations

www.charitylaw.ca www.carters.ca

20

- Incident response plans should be tested/drilled to develop skills, identify gaps and weaknesses and team members should practice/be trained so that they are able to respond appropriately to incidents
- Incident response plans should be reviewed and updated annually

"No plan survives contact with the enemy" – Helmuth von Moltke the Elder (19th century Prussian field marshal)

www.charitylaw.ca www.carters.ca

21

I. RESPONDING TO A PRIVACY BREACH

- In the event of a privacy breach, the following steps should be taken in accordance with the incident response plan:

1. Containment

- Take immediate action to:
  - Stop the breach
  - Retrieve and secure any personal information that was collected, used or disclosed without authority
  - Prevent further breaches by *e.g.* shutting down the system that was breached, changing passwords, revoking access

www.charitylaw.ca www.carters.ca

22

2. Investigation

- Designate an investigation lead or team
- Investigate and document the breach
- Determine (not exhaustive):
  - The cause and extent of the breach
  - How many individuals were affected by the breach?
  - Who was affected by the breach: Staff, donors, clients, others?
  - What personal information was involved, how much personal information was involved, how sensitive was the information *e.g.* health or financial information

www.charitylaw.ca www.carters.ca

23

- Is the information encrypted or otherwise not readily accessible?
- What steps have already been taken to minimize the harm?
- Is there a risk of significant harm to individuals (*e.g.* bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property)?
- Is there a risk to the organization?
- Is there a risk of ongoing or further breach?

24

3. Notification

- Report and escalate to internal personnel/teams immediately upon discovery of the breach
- If the organization is subject to PIPEDA or if it chooses to voluntarily comply with PIPEDA, report to the OPC and notify the affected individual as soon as feasible after you have determined that a breach of security safeguards involving a "real risk of significant harm" to an individual has occurred
- Direct notification (*e.g.* mail, email, or telephone) is required except in limited circumstances

25

- The notification must include enough information to allow the individual to understand the significance of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or mitigate the harm. Notices must contain the information set out in the regulations
- It may be appropriate to notify others of the breach such as the police, credit card companies, banks, credit reporting agencies or insurers
- If the organization is a health information custodian subject to Ontario's *Personal Health Information Protection Act,* notify the affected individual of the breach at the first reasonable opportunity and report to the IPC regarding privacy breaches
- If you are caught by the laws of another jurisdiction there may be other reporting obligations *e.g.* Alberta, GDPR (EU)

26

4. Prevention of Future Breaches

- Determine:
  - If there are systemic issues that need to be corrected, *e.g.* gaps in security, inadequate contracts with third party vendors
  - If follow up or remedial action is necessary *e.g.* improved training, employee discipline
  - If new or amended privacy policies are required
  - If a security audit is required
- Develop a plan to prevent future breaches

27

J. LEGAL PRIVILEGE FOR PRIVACY BREACH INVESTIGATIONS

- Solicitor-client privilege applies to confidential communications between a lawyer and client for the purpose of seeking or giving legal advice
- Documents that are subject to legal privilege do not have to be disclosed to third parties unless privilege is waived
- It could be beneficial for an organization responding to a privacy incident to retain legal counsel so that it is able to establish legal privilege over sensitive documents and communications, where appropriate, such as those revealing gaps and deficiencies
- It is advisable to retain legal counsel as early as possible

28

- The burden is on the party claiming the privilege to prove that it applies
- External counsel can also retain, direct and supervise other experts, for expressly stated legal advice or litigation purposes, and receive their reports, in order to establish privilege
- Care must be taken not to inadvertently waive privilege through *e.g*. communication with third parties

29

K. OTHER EXPERT ADVISORS

- In addition to legal counsel, an organization may find it necessary or advisable to engage (possibly through counsel) other expert advisors including:
  - IT forensic specialists
  - Public relations/communications specialists
  - Investigators
- Organizations should also consider obtaining cyber insurance that could cover costs of incident response, legal and other advice and even the cost of ransom in some cases

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001
Ottawa Toronto Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca