What is Your Privacy and Cybersecurity Electronic Quotient (EQ)?

Hosted by the Ontario Regional Council

June 20, 2018

Albany Club

Toronto, ON

ACPM Privacy & Cybersecurity
A Legal Primer

Dan Michaluk

Partner

Hicks Morley Hamilton Stewart Storie LLP

Custodianship, Duty and Standard

- One who takes custody of personal information has a duty to take reasonable steps to see that it is handled as authorized and not lost or stolen

Statutory duties – or lack thereof?

- Employers in Ontario
  - Federally regulated employers are regulated directly by PIPEDA in respect of their employees
  - Believe it or not, no other Ontario employers are subject to privacy legislation

Statutory duties – or lack thereof?

- Do third-party administrators (who are paid fees for service) attract PIPEDA regulation?
  - It's complicated and uncertain
  - The New Brunswick State Farm case gives the argument for non-application
  - Many employers and administrators take the position PIPEDA applies

Common law fills the gaps anyway

- Data breach claims are based in
  - Negligence
  - Contract
  - Privacy torts

The standard of care

- Reasonable safeguards (watch your promises to “ensure”)
  - Technical, administrative and physical
- The standard is set based on all the circumstances (standards do not dictate)
- Proof of due diligence support a regulatory defence and can help you demonstrate that you met the standard of care

Elements of a privacy and security program

- Addressed by recent OPC findings in Ashley Madison and Vistek
  - Favour formalization and documented procedures
  - Have regular and documented risk assessments
  - More robust monitoring and logging
  - Strong and formalized incident response process

Outsourcing due diligence

- Make sure you address all three elements
  - Vendor selection
  - Contracting
  - Administration
- Hot spots in contracting
  - Do you have the control you need to respond to an incident?
  - Are your audit rights too strong for you to live up to?

Notification of incident

- In November we will have PIPEDA breach notification
  - “Breach of security safeguards”
  - Notification based on a “real risk of significant harm”
    - Identity fraud = significant harm
    - Real risk ≠ probable
  - Even if PIPEDA does not apply, expectations are changing

ACPM Privacy & Cybersecurity
A Legal Primer

Dan Michaluk

Partner

Hicks Morley Hamilton Stewart Storie LLP

What is Your Privacy and Cybersecurity Electronic Quotient (EQ)? Pension Law Considerations

Adam Ngan
Associate
Blake, Cassels & Graydon LLP
June 20, 2018

Legal Framework

- The *Pension Benefits Act* (PBA) does not expressly impose obligations on pension plan administrators regarding cyber security or privacy
- Such obligations come as a result of fiduciary duties under the PBA, aka the "Prudent Person Rule", which apply in addition to other legal requirements

Plan Administrator Fiduciary Duties

Statutory Duty of Care (PBA)

s.22(1)

- the administrator of a pension plan shall exercise the care, diligence and skill in the administration and investment of the pension fund that a person or ordinary prudence would exercise in dealing with the property of another person

s.22(2)

- the administrator of a pension plan shall use in the administration of the pension plan and in the administration and investment of the pension fund all relevant knowledge and skill that the administrator possesses, or by reason of the administrator's profession, business or calling ought to possess

Common Law Duties

The fiduciary concept

- a fiduciary stands in a position of trust to another individual
- a fiduciary must act in a manner consistent with the best interests of the beneficiary
- the actions of the fiduciary will be viewed with a strictness unknown to most other areas of law

Primary Duties of a Fiduciary

Duty of Loyalty / Good Faith

- fiduciary must act towards the beneficiary with a heightened sense of loyalty, fidelity and even-handedness
- avoidance of potential conflicts of interest

Duty of Care

- demonstrate a level of care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances

Primary Duties of a Fiduciary *(cont'd)*

Duty of Prudence

- about process, not results – ensure that prudent and thoughtful consideration goes into all decisions
- key is whether appropriate steps taken in decision-making process
- essential elements in pension context:
  - establishing and supervising an appropriate plan administration structure
  - good faith reliance on professional advice may be permitted subject to terms of governing documents and reasonableness

Delegation to Agents

PBA permits plan administrators to delegate to agents, but administrator still retains ultimate fiduciary duty

- PBA, s. 22(5) – where it is "reasonable and prudent in the circumstances so to do"
- PBA, s. 22(7) – administrator is responsible for agent
- PBA, s. 22(8) – agent is subject to same standards as administrator

Pension Plan Electronic Records and Communications

- Annual/biennial statements, PBA s. 27
- Termination/retirement statements, PBA s. 28
- Member and other beneficiary disclosure of information/access to records, PBA s. 29
- Electronic communications from administrators to plan beneficiaries expressly permitted in compliance with the *Electronic Commerce Act, 2000*, PBA s. 30.1

Regulator Guidance

FSCO Policy A300-200 re implementation and maintenance of prudent record keeping practices

- Expressly recognizes electronic record storage
- FSCO's expectations for different categories of information and other considerations, e.g., admissibility under the *Evidence Act*

FSCO Policy A300-806 and CAPSA Guideline #2 re electronic communications

Regulator Guidance*(cont'd)*

Importance of Cyber Security, FSCO statement, October 2016

- cybersecurity policies should comply with legislation and take into account size and complexity of "business" (pension plan)
- cybersecurity procedures and practices to be reviewed regularly for relevance, effectiveness
- obtain professional advice

Other FSCO commentary more focused on plan member perspective

Cyber Security Considerations

- Plan administrator responsible for creation and maintenance of plan records
- FSCO policy requires administrator to implement and maintain prudent record keeping practices
- Plan administrator must comply with applicable law, including privacy laws, which require appropriate safeguards

Cyber Security Considerations

(cont'd)

- Plan records typically contain substantial personal information about plan members, their spouses and beneficiaries
- Information maintained in respect of pension fund includes financial information about employer, fund investments and possibly banking information of members (e.g., where fund holder acts as paying agent)

Cyber Security Considerations *(cont'd)*

- Records may be created and maintained by third parties
  - service providers
  - fund holder
- Administrator is ultimately responsible for operation of plan and fund, including plan records, subject to potential legal recourse against third parties

Best Practices

- Compliance checklists
- Governance reviews, including appropriate delegation/supervision and processes for plan administration
- Reviews of third-party service provider agreements, due diligence
- Periodic updates
- Personnel and plan member training
- Cybersecurity insurance

What is Your Privacy and Cybersecurity Electronic Quotient (EQ)?

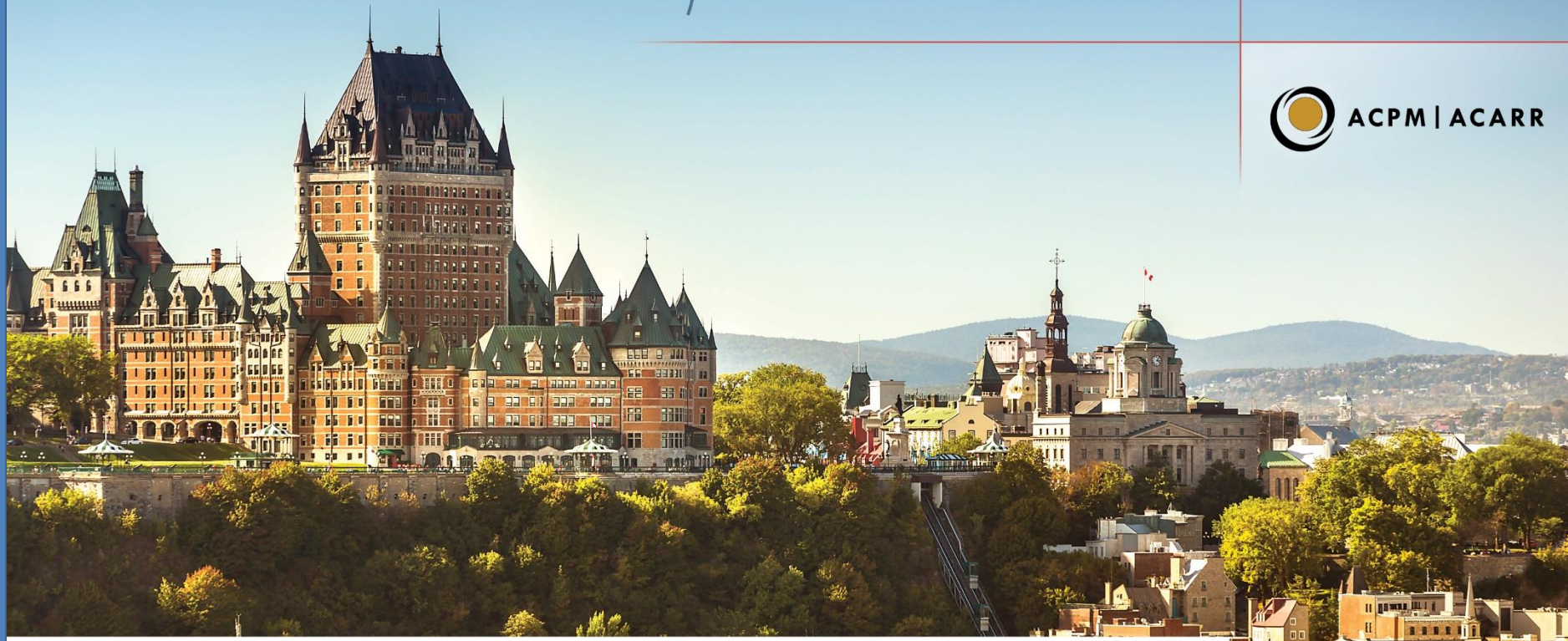
Steven Hurley
Manulife

The Next 150

FORTIFYING RETIREMENT FOR THE FUTURE

2018 ACPM NATIONAL CONFERENCE

ACPM | ACARR



Québec City, QC

Fairmont Le Château Frontenac

SEPTEMBER 11–13, 2018

www.acpm.com

DIAMOND SPONSOR ›

Desjardins Insurance
Life • Health • Retirement

Starting with a global perspective, the 2018 ACPM National Conference will provide strategic insights for the retirement industry now and in the future.