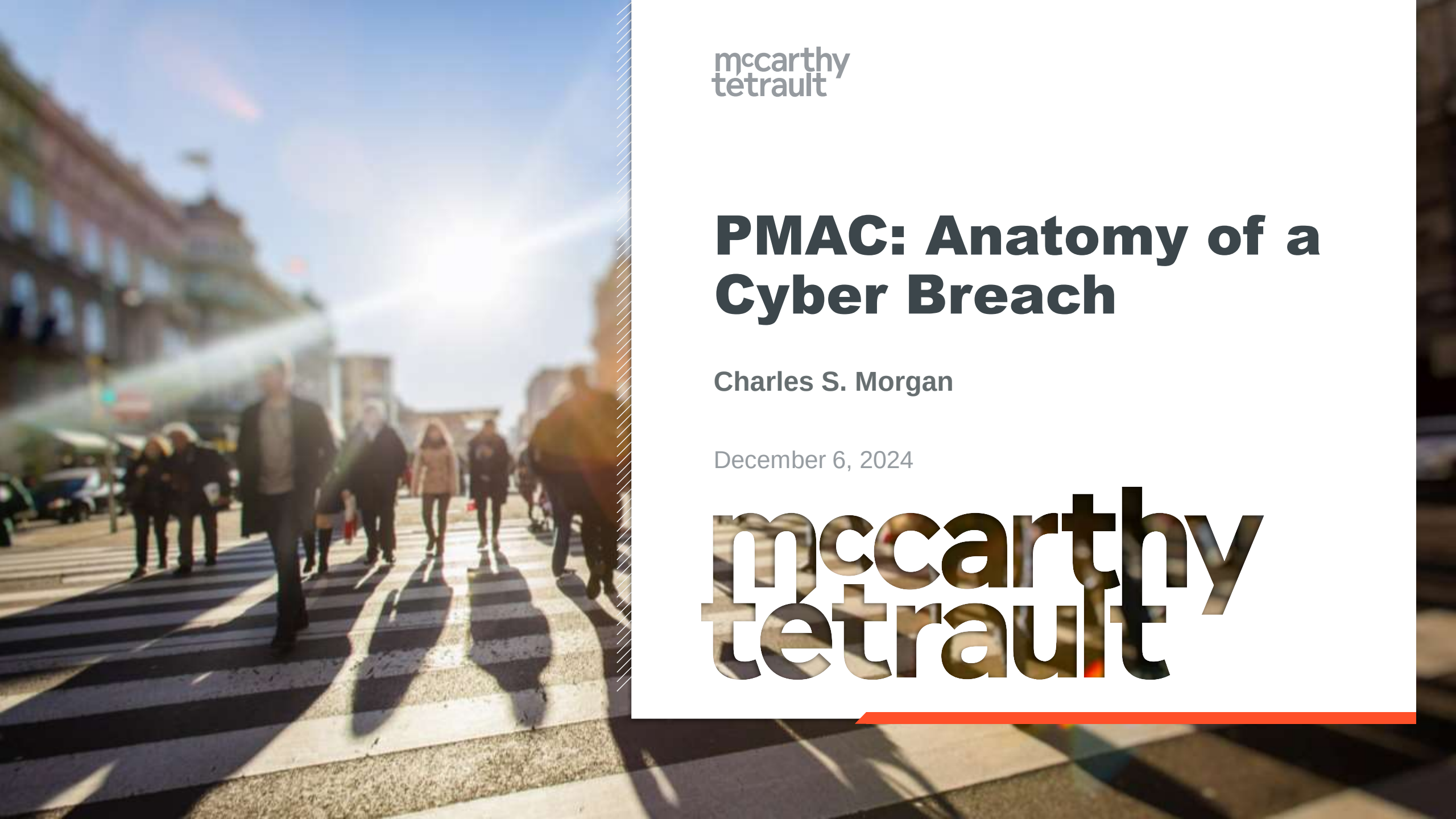


mccarthy tetrault

PMAC: Anatomy of a Cyber Breach

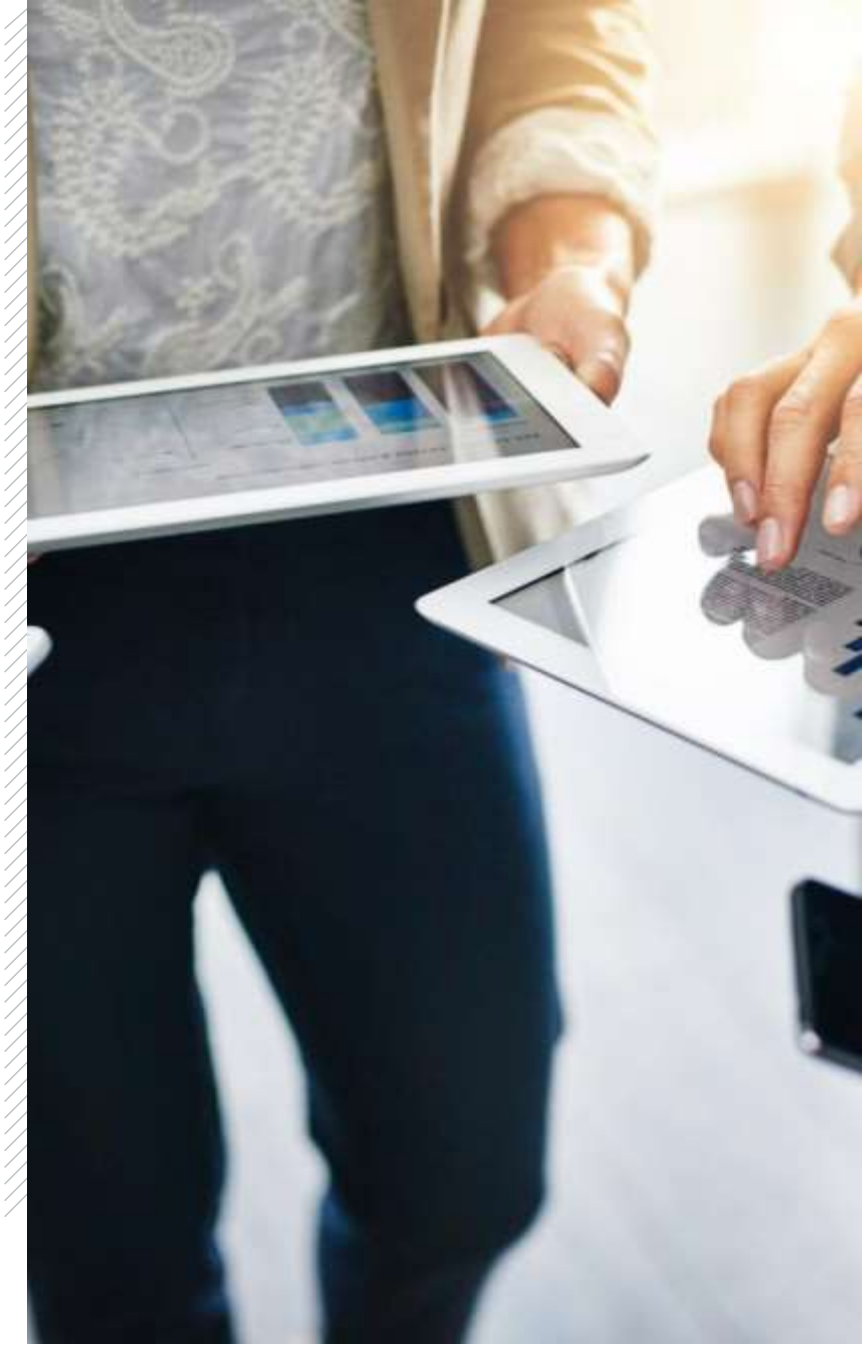
Charles S. Morgan

December 6, 2024

mccarthy tetrault

Agenda

- Cyber Readiness
- Cyber response
  - Managing privilege
  - Managing a cyber response team
  - Factors to consider when responding to a ransom request
  - Breach notification obligations and communications protocols



mccarthy tetrault

1. Cyber Readiness

Understanding the Evolving Threat Landscape

—Ransomware + Data Exfiltration + Extortion

—« Man in the middle »

—State-sponsored threat actors

—Ransomware-as-a-Service

—Deep Fakes: the new frontier

Pre-Planning Incident Response

—**Data inventory:** know how personal information flows through your organization and through the hands of key service providers

—**Cyber incident response plan:** have an *actionable* step-by-step plan for addressing incidents (with accountable parties)

—Prepare **template incident log** aligned with record retention rules (bearing in mind privilege concerns)

—Prepare **template notification letters** aligned with notice requirements

Incident Response Playbook

—Framework for assessing potential for “real risk of significant harm” (or “RROSH”) and recording the assessment in a way that minimizes privilege risks

—Detailed but **actionable** step-by-step plan for addressing incidents, including stopping incident, escalation to external advisors, insurance notices, recovering data, remediation of immediate issue and collateral issues

—Can be tiered to differentiate between minor and major incidents

—Should account for all applicable laws → is clock ticking on notice to regulators?

—Regular table-top exercises and debriefs allow you to stress-test and update procedures

mccarthy tetrault

Insurance

—Have insurance experts who will advise on what steps should be taken with regards to the cyber insurance policy review, notifications and coordination with insurers

—Evaluate insurance policies to understand coverage for different types of incidents

—Use insurance as a risk management tool

The “Breach Coach”

- Scoping the breach (identifying affected information)
- Statutory notification and reporting obligations (to public, regulators)
- Maintaining privilege
- Hiring service providers (forensic investigators, ransom negotiators, e-discovery)
- Supervising the investigation
- Contractual obligations and indemnities
- Applicable sanctions/AML issues (ransomware demand)
- Litigation risk mitigation strategies (e.g., offering protection products)
- Cross-border implications
- Public company disclosure requirements
- Post-mortem

mccarthy tetrault

2. Cyber Response

Six Key Elements for a Cyber Response

1. Stop the bleeding: close the door, permanently.
2. Call on expert help: technical; legal; PR; GR.
3. The lawyers, and privilege, are important. But a fast, thoughtful response is job one.
4. Determine your story, and tell it consistently: to your customers, to the Regulators, to affected business partners, and later, if necessary, to the Court.
5. Be realistic: avoid overly optimistic statements, as they often come back to haunt you.
6. Learn your lessons: Regulators and the public expect companies to seriously assess the incident and make meaningful changes.

Escalation Criteria

—Understand and communicate incident life cycle management within the organization

—Establish criteria and process to evaluate and escalate an incident to senior management

—Incorporate and document RROSH assessment

Fact Gathering and Preservation

—Determine which steps should be taken to preserve evidence (litigation hold) → duty triggers when litigation reasonably foreseeable

—Tension between destroying potentially probative evidence and fixing the problem

—Record preservation obligations could include preventing files from being deleted, enhanced monitoring of the network, and suspending logs and backup tapes from being overwritten

—Specialized technical solutions should be used to preserve, collect and analyze evidence (*e.g.*, MT>3)

—Litigation counsel, forensics and technical experts (*e.g.*, MT>3) should review a plan collaboratively to mitigate potential negative outcomes

Considerations for Ransom Payment

1. Who is attacking you?
2. How much data did they get? How sensitive is that data?
3. Is the decryption key certain to work?
4. Is the threat actor on a sanctions list?
5. What are the costs of not paying?
6. What is my timeline for all scenarios?

Considerations for Forensic Reports

1. What is the current case law?
2. Why do I need a report? Who needs to see it?
3. Who is creating the report?
    a. Do I have a pre-existing relationship with them?
    b. Were they on the ground before any lawyers?
    c. Remediation versus forensic analysis – *two firms?*
4. What story do we expect the report to tell?
5. A plea for version control.

Privilege Strategy

—Involve external counsel at the outset and throughout response

—Be mindful of in-house counsel roles; business advice is not privileged

—Plan a communication strategy ahead of time; be intentional about what gets put in writing; identify the need-to-know “inner circle” and include legal counsel

—External counsel should retain and oversee third parties investigating the breach for the purpose of providing legal advice; negotiate third party retainers in advance

—Consult counsel before disclosing privileged documents outside the organization (e.g., to regulators); try to limit waiver where disclosure is necessary

—Ensure documentation reflects applicable privileges (e.g., privilege labels)

Breach Notification + Mitigation

— Applying the RROSH test

—Which jurisdictions?

—How, When and Whom to Notify?

—Obligations to notify clients? Business partners?

—Obligations to mitigate harm – credit monitoring?

—Issuance v. redemption pricing

mccarthy tetrault

Questions?

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite MZ400
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

NEW YORK

55 West 46th Street, Suite 2804
New York NY 10036
UNITED STATES
Tel: 646-940-8970
Fax: 646-940-8972

LONDON

1 Angel Court, 18th Floor
London EC2R 7HJ
UNITED KINGDOM
Tel: +44 (0)20 7786 5700
Fax: +44 (0)20 7786 5702

mccarthy tétrault

PMAC: Implementing a Pan-Canadian privacy compliance program consistent with Quebec's Law 25

Charles Morgan

December 4, 2024

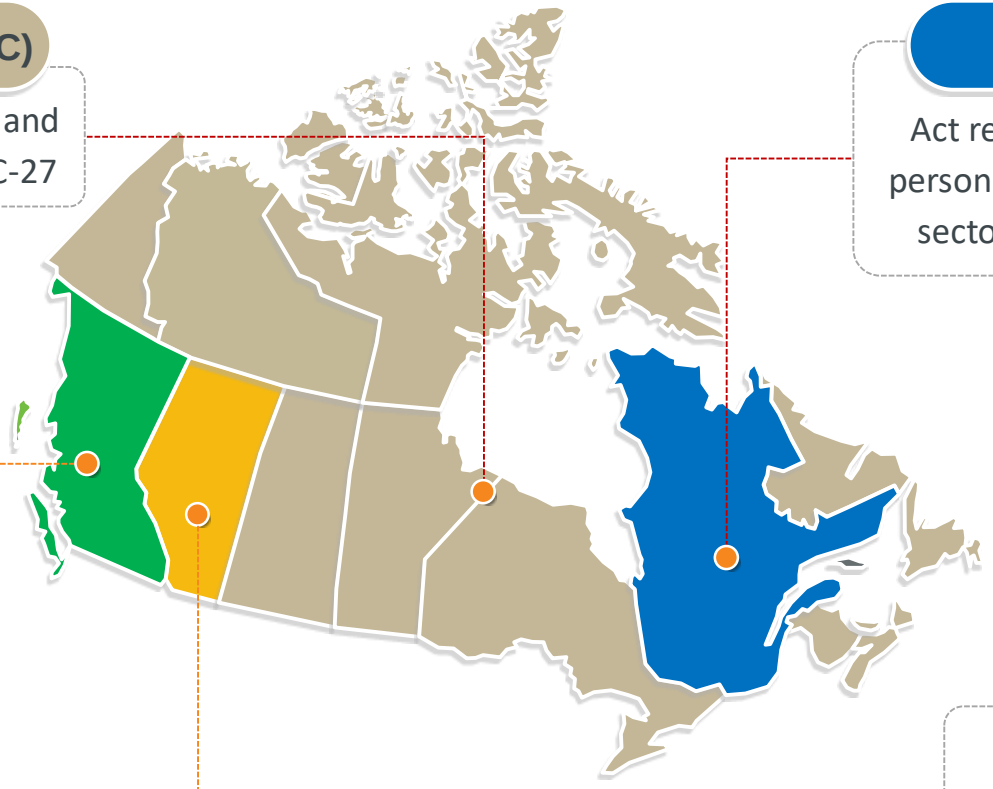
mccarthy tétrault

1. Privacy Legislative Update – CPPA
2. Law 25 – Québec: the distinct society!
3. Lessons Learned from Recent Commissioner Findings
4. Implementing a Compliance Program

Canadian Landscape: Private Sector Privacy*

Canada (except AB, BC, QC)

Personal Information Protection and Electronic Documents Act / Bill C-27



Quebec

Act respecting the protection of personal information in the private sector (as amended by Law 25)

British Columbia

Personal Information Protection Act

Alberta

Personal Information Protection Act

* Each province also has a health sector privacy law that only applies to personal health information

CPPA – Overhaul of federal privacy law

mccarthy tétrault

Federal Privacy Reform

See McCarthy Tétrault's Bill C-27 Blog Series for additional details

—Privacy regulation is undergoing a shift from "name and shame" to **a law with teeth**.

—**Bill C-27** proposes three new pieces of legislation:

- Consumer Privacy Protection Act ("**CPPA**");
- Personal Information and Data Protection Tribunal Act ("**PIDPTA**"); and
- Artificial Intelligence and Data Act ("**AIDA**").

—The CPPA and AIDA must be taken seriously. CPPA imposes fines of up to the greater of $25,000,000 and 5% of the organization's annual gross global revenue. AIDA provides for fines of the greater of $10,000,000 and 3% of the person's annual gross global revenue.

—CPPA also contains a **problematic private right of action** that can be weaponized in class actions.

—Doubtful that Bill C-27 will be adopted.

Law 25 – Quebec: the distinct society!

mccarthy tétrault

It is fully in force!

Sept 22, 2021:

Royal assent

Sept 22, 2022:

Sections on confidentiality incident notification obligations and the appointment of persons in charge of protecting personal information

Sept 22, 2023:

Majority of the sections (incl. penalties, developing privacy policies and practices, changes in consent requirements, etc.)

Sept 22, 2024:

Right to portability

New Sanctions

Administrative Monetary Penalties

- For failures to inform, collection and communication of personal information in contravention of the act, failure to report confidentiality incidents, and failure to take appropriate security measures to protect personal information.
- Potential for an undertaking with the CAI to remedy the default, and avoid an administrative monetary penalty.
- Maximum of $10,000,000 or 2% of worldwide turnover for the preceding fiscal year, whichever is greater.

Penal Penalties

- Depending on the severity, frequency, and impact of non-compliance, the CAI may instead apply a penal penalty.
- Maximum of $25,000,000 or 4% of worldwide turnover for the preceding fiscal year, whichever is greater.

Comparison

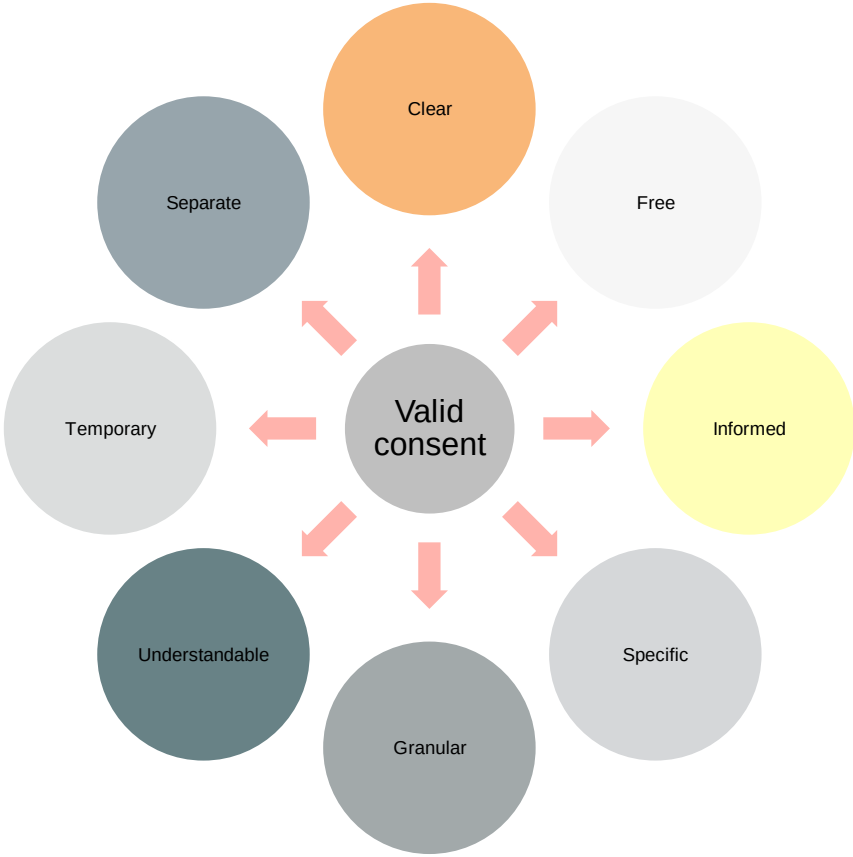
- Penalties for non-compliance with Bill 64 have the potential to be the most costly in Canada, as both PIPEDA and the Alberta PIPA impose penalties of up to $100,000 per violation.
- Bill 64's fines for non-compliance now more closely approximate those for GDPR non-compliance.

Consent

*"Consent under this Act must be **clear**, **free** and **informed** and be given for specific purposes [i.e. **Specific**]. It must be requested for each such purpose [i.e. **Granular**], in clear and simple language [i.e. **Understandable**]. If the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned [i.e. **Separate**]. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested [this is another aspect of consent being **Informed**].*

The consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor 14 years of age or over is given by the minor, by the person having parental authority or by the tutor.

*Consent is valid only for the time necessary to achieve the purposes for which it was requested [i.e. **Temporary**].*



See: Lignes directrices 2023-1 sur les critères de validité du consentement (quebec.ca)

Privacy Impact Assessments

Privacy impact assessments must be conducted on the **design or implementation of an information system:**

— Section 3.3:

> "Any person carrying on an enterprise must conduct an assessment of the privacy-related factors of any project of acquisition, development and redesign of an information system project or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information."

- Section 17 - Privacy impact assessments must be conducted **when communicating personal information outside of Québec:**

> "Before communicating personal information outside Québec, a person carrying on an enterprise must conduct an assessment of privacy-related factors. The person must, in particular, take into account
>
> (1) the sensitivity of the information;
>
> (2) the purposes for which it is to be used;
>
> (3) the protection measures, including contractual ones, that would apply to it; and
>
> (4) the legal framework applicable in the State in which the information would be communicated, including the data protection principles applicable in the foreign State including the legal framework's degree of equivalency with the personal information protection principles applicable in Québec."

Communication to Third Parties

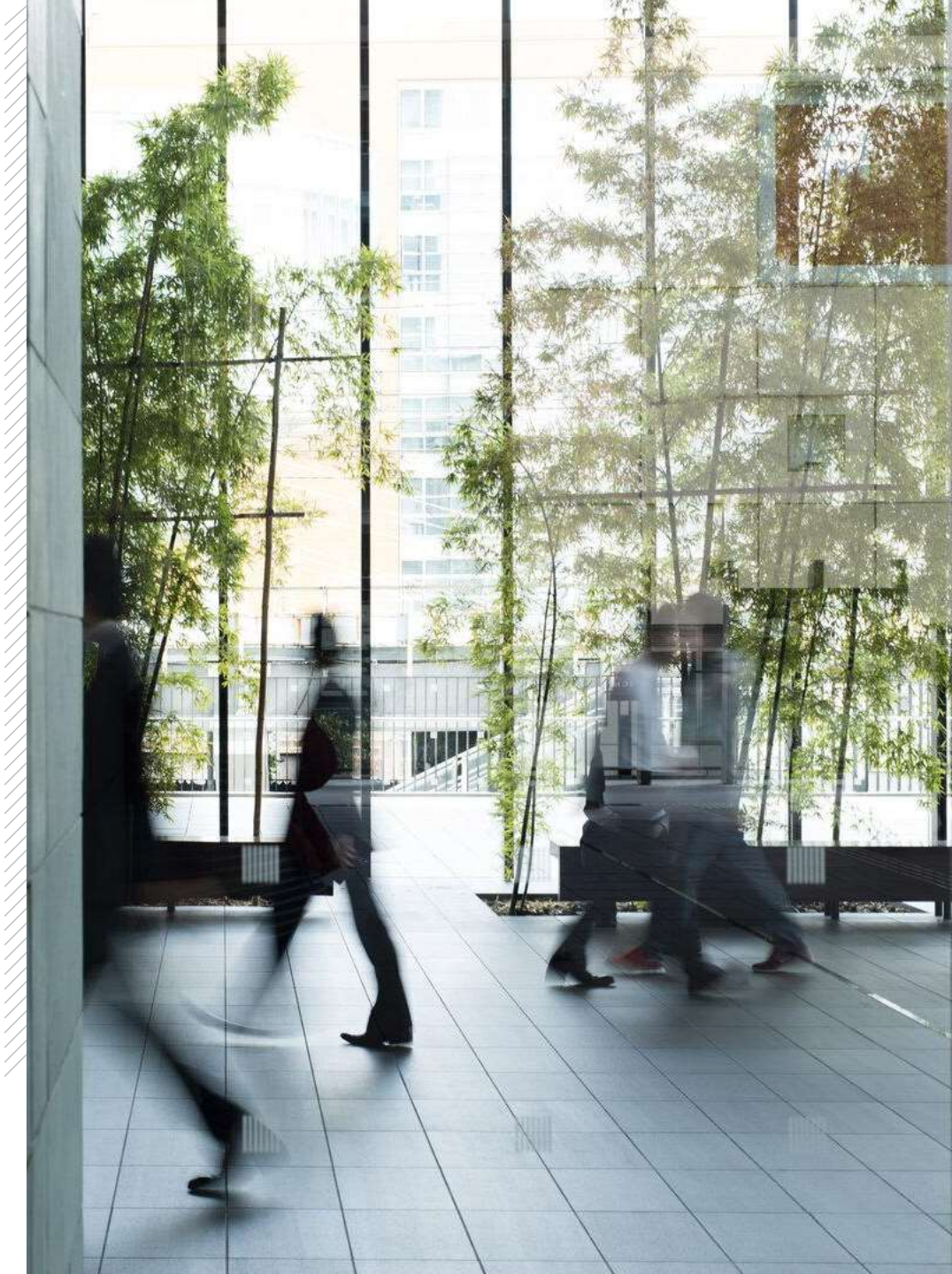
Communication of personal information to service providers or contractors must contain **protective measures to guarantee privacy protections**

Specify in the mandate or contract (Section 18.3):

— the measures the mandatory or the person performing the contract must take to protect the confidentiality of the personal information communicated

— ensure that the information is used only for carrying out the mandate or performing the contract

— ensure that the mandatary or person does not keep the information after the expiry of the mandate or contract.



Considerations for Biometrics Disclosure

— 44. **A person's identity** may not be verified or confirmed by means of a process that allows **biometric characteristics or measurements** to then be used except where such verification or confirmation has been **previously disclosed to the Commission d'accès à l'information** and except with the **express consent** of the person concerned. Only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not then be used without the person's knowledge may then be used for identification purposes.

— 45. The creation of a database of biometric characteristics and measurements **must be disclosed to the Commission d'accès à l'information promptly and not later than 60 days before it is brought into service**.

1. Are you using biometrics for the purpose of identification?
2. Is the use of biometrics optional? Express consent?
3. What rôle(s) do you play in the creation and operation of the biometric database?
4. Can you justify your use of biometrics?
    - Necessity
    - Proportionality
    - Security

Privacy by default

— 8.1 In addition to the information that must be provided in accordance with section 8, any person who collects personal information from the person concerned using technology that includes functions allowing the person concerned to be identified, located or profiled must first inform the person(1) of the use of such technology; and

— (2) of the means available to activate the functions that allow a person to be identified, located or profiled.

— “Profiling” means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour.

— 9.1. Any person carrying on an enterprise who collects personal information when offering a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned.

— The first paragraph does not apply to privacy settings for browser cookies.

Data Portability

In force as of September 2024, the right to portability allows any citizen to obtain the **computerized** personal information **collected from them** in a **structured, commonly used, and technological format**

— **Computerized**: The right to portability applies only to computerized (not paper-based) personal information.

— **Collected from you**: The computerized personal information must have been collected directly or indirectly from you by a public body or a company. Indirectly collected information includes data generated by your activities, such as your purchase history, travel records, driving habits, etc.

— Data portability right **does not apply to information that has been generated or inferred** by the public body or company: i.e. generated by analysis, observation, or obtained through algorithms and correlations

— A format is considered "**structured and commonly used**" when commonly used software applications can easily recognize and extract the information it contains (e.g. CSV file).

— Companies are required to ensure that **any new project involving the acquisition, development, or overhaul of an information system** or electronic service provision **allows for the communication of computerized personal information in a structured and commonly used technological format**

— An individual can also request that their **computerized personal information be communicated in a structured and commonly used technological format to an authorized person or company**.

Lessons from Recent OPC Decisions

mccarthy tétrault

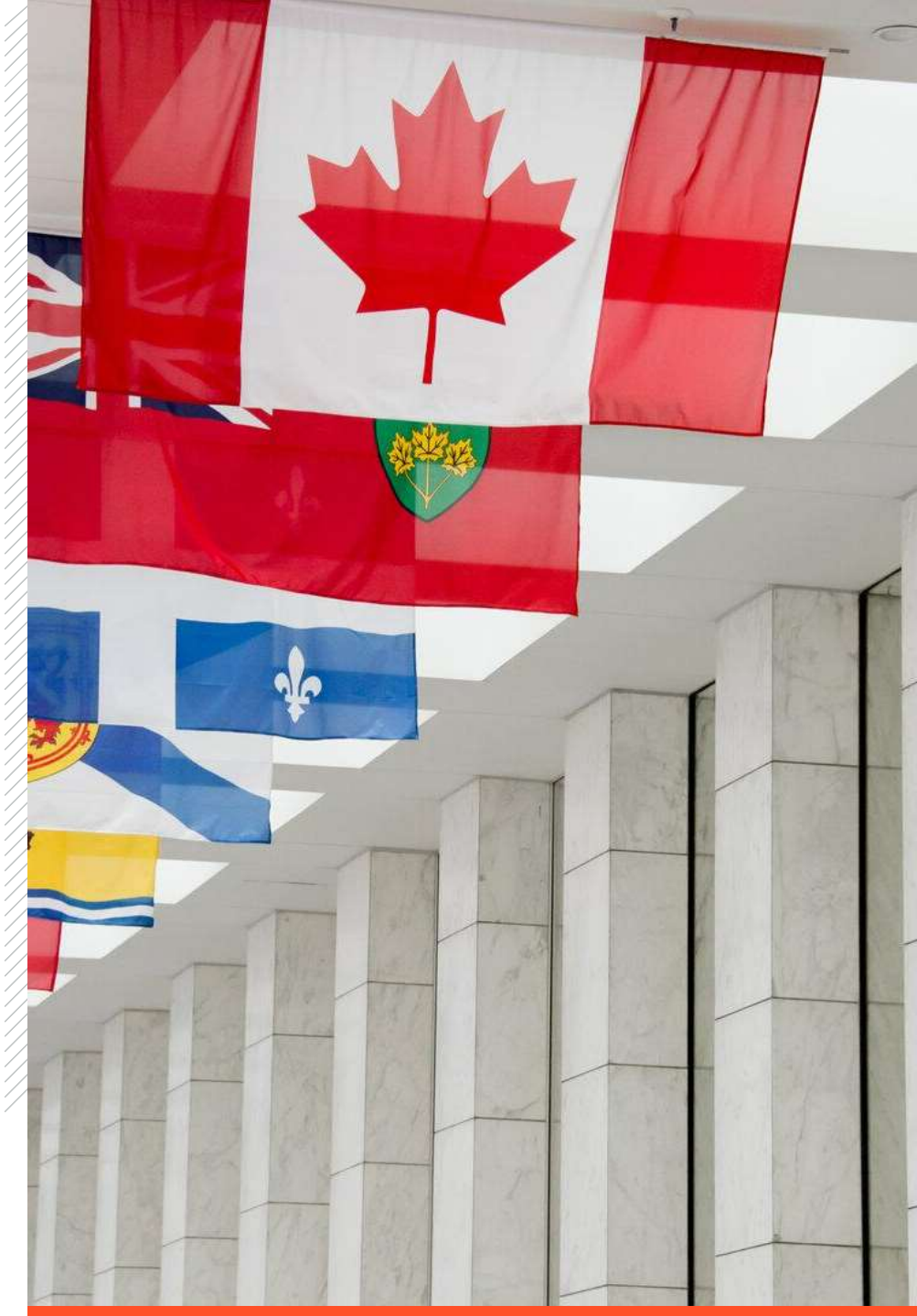
Tim Hortons Decision (2022)

—OPC found that Tim Hortons did not have a legitimate need to collect vast amounts of sensitive location information where it never used that information for its stated purpose

—The consent obtained was invalid because Tim Hortons did not disclose that the app would track their location even when the app was closed, and made false statements to the contrary

—Contract terms with third party service provider were inadequate and would have allowed third party to use the information for its own purposes. Did not matter that the third party did not actually use the data that way

—Broader lack of accountability indicated by collection of data that Tim Hortons never used for the stated purpose and lack of privacy assessments “at key decision points”



mccarthy tetrault

Home Depot Decision (2023)

- OPC concludes that Home Depot did not obtain valid meaningful consent to share summary purchase information with Meta for the purpose of measuring the effectiveness of Facebook ads and Meta's own purposes.

  > "Home Depot did not provide any explanations, at this point-of-sale, regarding how it would use or disclose customer information for purposes other than to send them an e-receipt. Given the nature of the use and disclosure in question, as described above, this information would have been material to the customers' decision whether or not to provide their email address to obtain an e-receipt"

- OPC also suggests that Home Depot did not obtain sufficient consent to use customer information for its own marketing and analytics purposes because "the Privacy Statement uses **generic and vague** terms such as "improve our products and services".

- OPC disregards **non-sensitive nature** of information shared

mccarthy tetrault

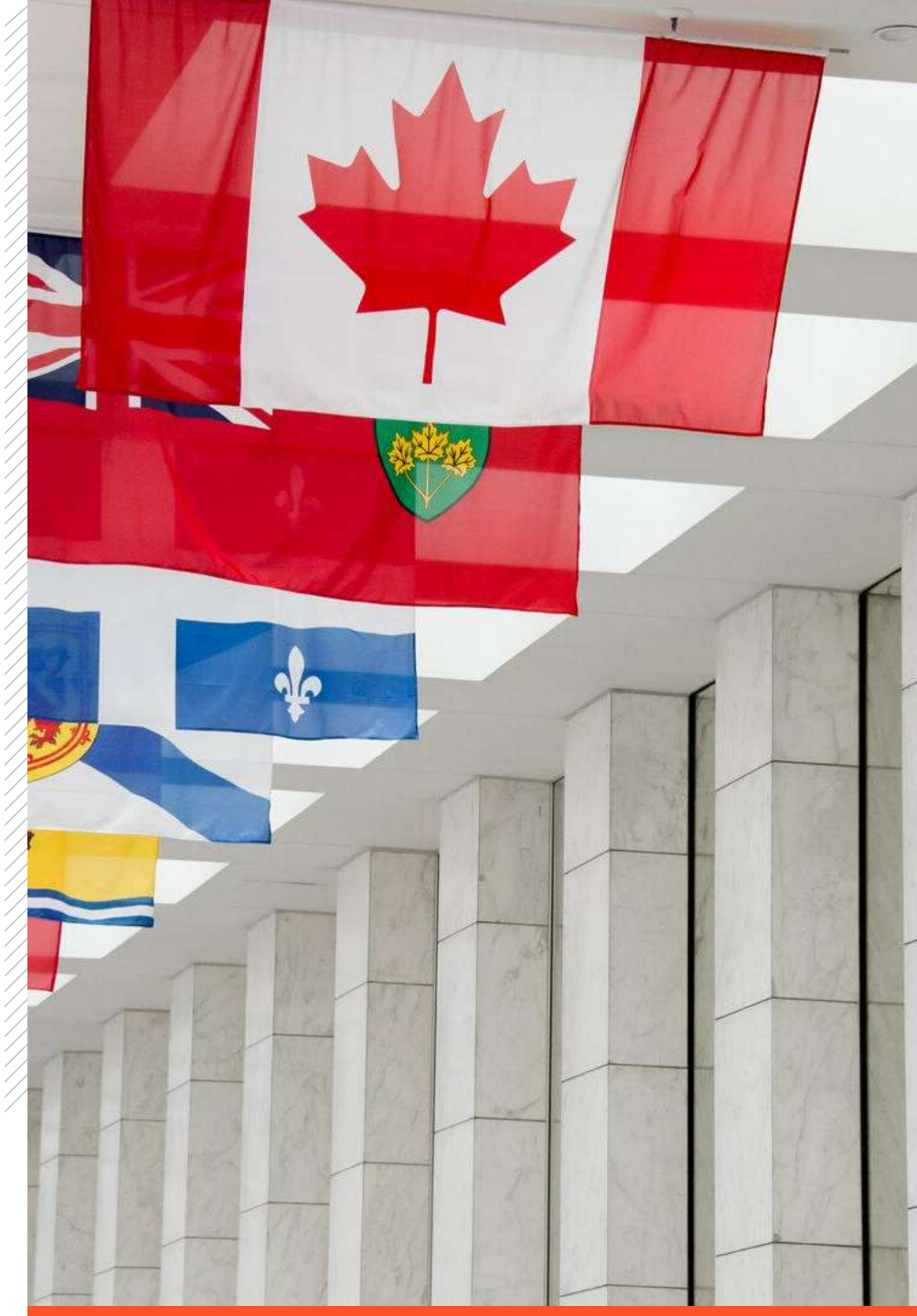
Facebook Decision (2023)

- OPC found Meta did not obtain meaningful consent from users whose personal information was shared with third parties, and did not adequately safeguard users' personal information from unauthorized collection, use, and disclosure by third-parties

- Commissioner applied to Federal Court for orders requiring Facebook make operational changes and to submit to ongoing supervision by the Commissioner and the court. The proposed supervisory order drew inspiration from a 2020 consent order between Meta and the U.S. FTC that gave a third-party assessor powers to monitor and report on Meta's compliance

- Federal Court found the Commissioner failed to prove lack of meaningful consent or failure to adequately safeguard users' personal information under PIPEDA.

- **Duty to safeguard information ends when the information is lawfully provided to the third party**



Implementing a Compliance Program

mccarthy tétrault

Phase 1: Current State Assessment

—Confirm jurisdictional scope of review

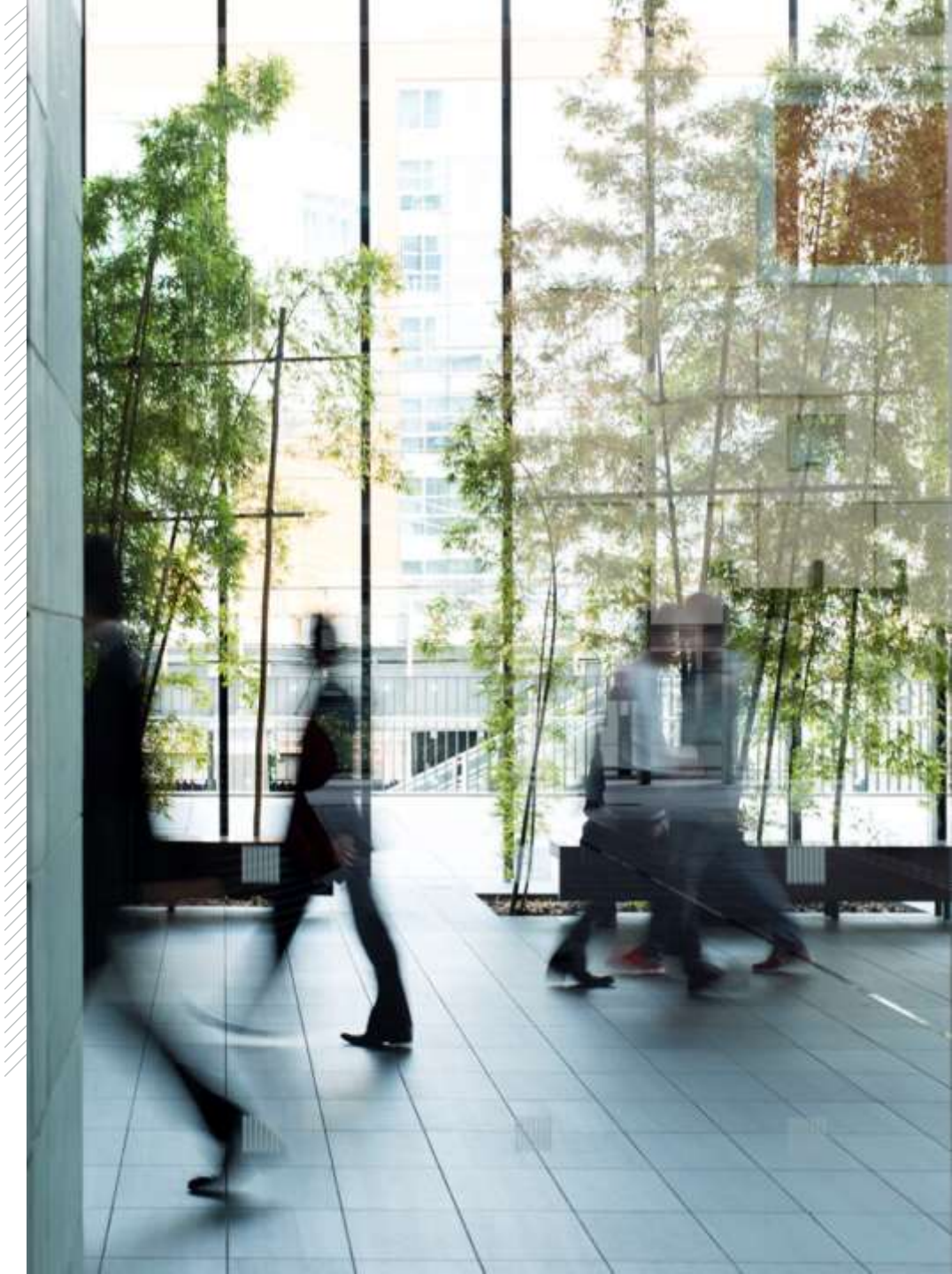
—Identify the team

—Prepare the tools

  —Document Review

  —Data Inventory

  —Compliance maturity analysis



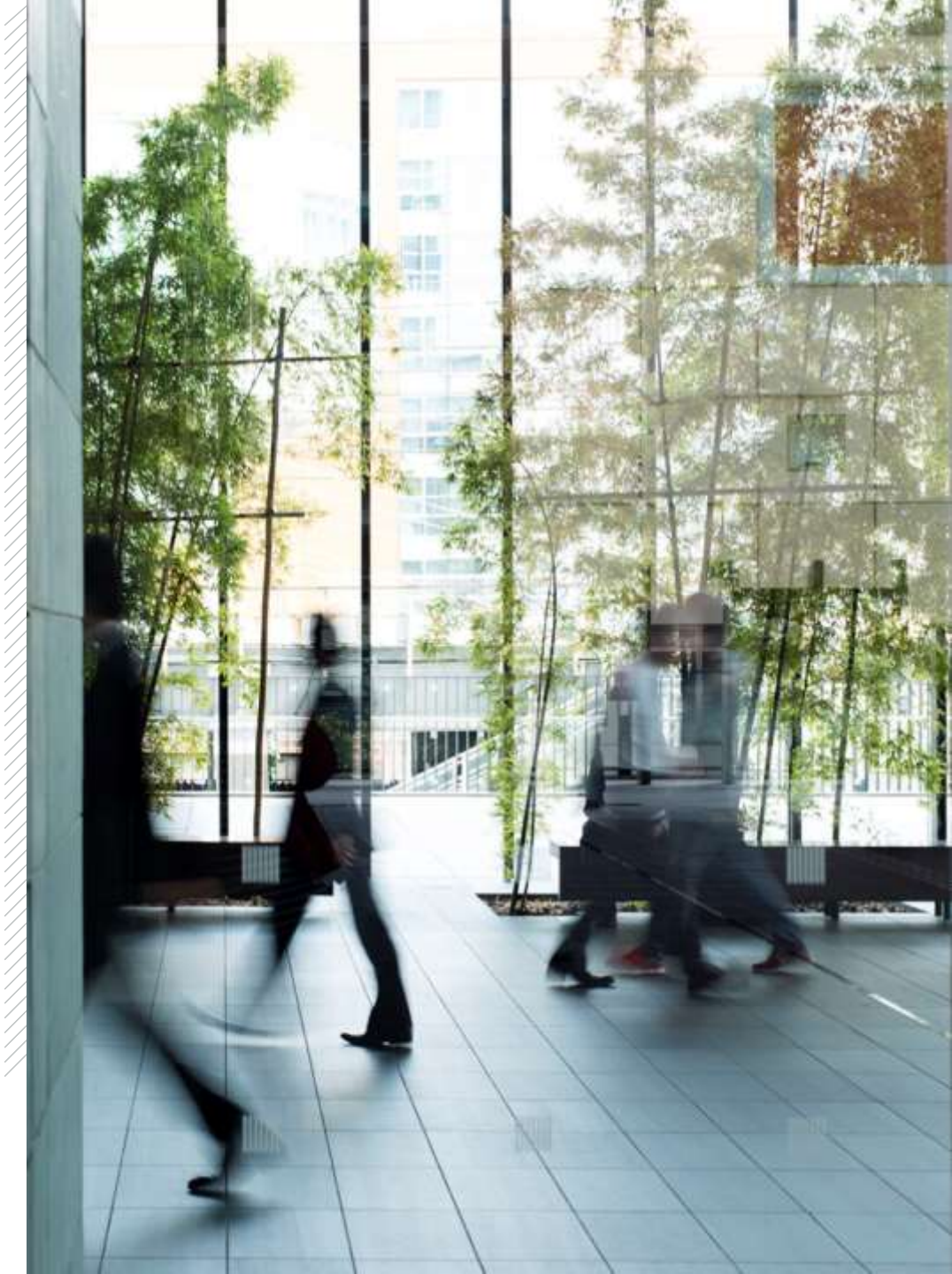
mccarthy tetrault

Phase 2: Gap Assessment

—Benchmarks upon which to base gap assessment

—Principles and controls

—Risk and priority categorization of gaps



Phase 3: Compliance Roadmap

— Risk Tolerance

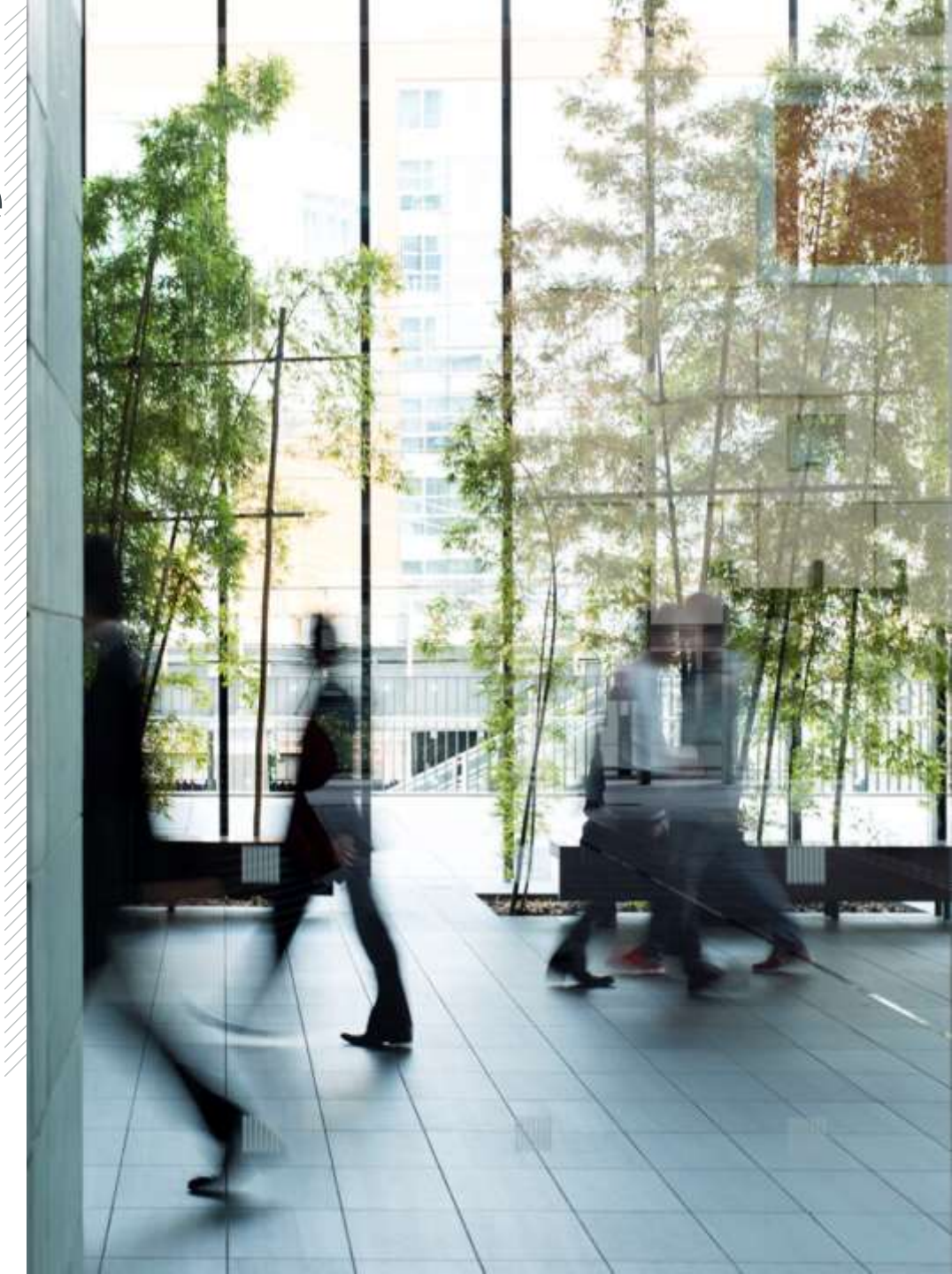
— Legislative timeline

— Compliance Budget

— Project Dependencies

— Quick wins

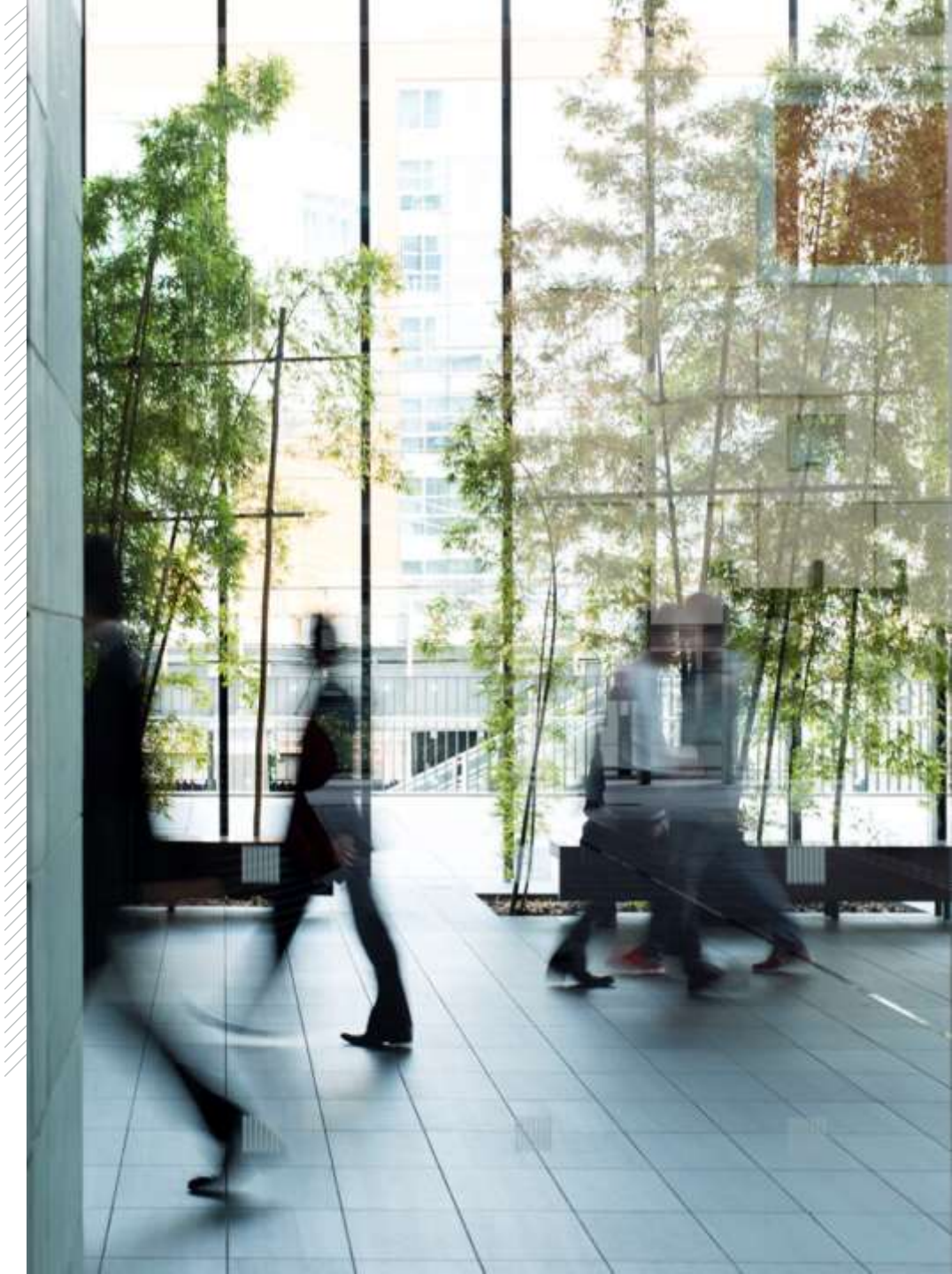
— Automation



mccarthy tetrault

Phase 4: Implementation

- Identifying affected projects and dependencies
- Policies, procedures and execution
  - Naming a CPO and building a team
  - Internal Privacy Framework + processes
  - PIA
  - Incident register
  - DPA and vendor management
  - Training
- Considering opportunities for automation



Questions?

cmorgan@mccarthy.ca

Use of Artificial Intelligence by Portfolio Managers

Sean D. Sadler and Shane C. D'Souza, with assistance from Mitch Spragg
McCarthy Tétrault LLP

December 4, 2024

Agenda

1. The Utility of AI
2. Current regulatory approach toward AI
3. Future regulatory direction
4. AI litigation and enforcement risks
5. AI Risk Mitigation Strategies

mccarthy tétrault

mccarthy tetrault

The Utility of AI

AI in the investment industry involves the use of machine learning, data analytics, and algorithms to enhance decision-making, automate processes, and optimize investment strategies. It enables more accurate market predictions, risk management, personalized financial advice, and automated trading. AI analyzes vast amounts of data to identify patterns and trends, helping investors make informed decisions faster and more efficiently, potentially outperforming traditional methods.

mccarthy tetrault

The Next Technology Frontier: Differences Between Traditional Software And AI

- Decision Making Process
- Data Analysis Capabilities
- Complexity and Flexibility
- Speed and Efficiency
- Personalization
- Cost and Accessibility

mccarthy tetrault

Promise of AI

IMPROVING CUSTOMER RELATIONSHIPS

- improve customer service
- find new clients
- (e.g. chat bots, using demographics like age, income level, and inflows and outflows of capital to optimize services such as personalized investment reports and educational content)

INCREASED EFFICIENCY

- automating pre- and post-trade processes (e.g., generation of trade reports and submissions to regulators)
- streamlining HR functions (e.g., screening candidates)
- summarizing KYC meetings
- initial drafts of marketing material

OPTIMIZE INVESTMENT RETURNS

- portfolio construction
- investment selection
- investment research

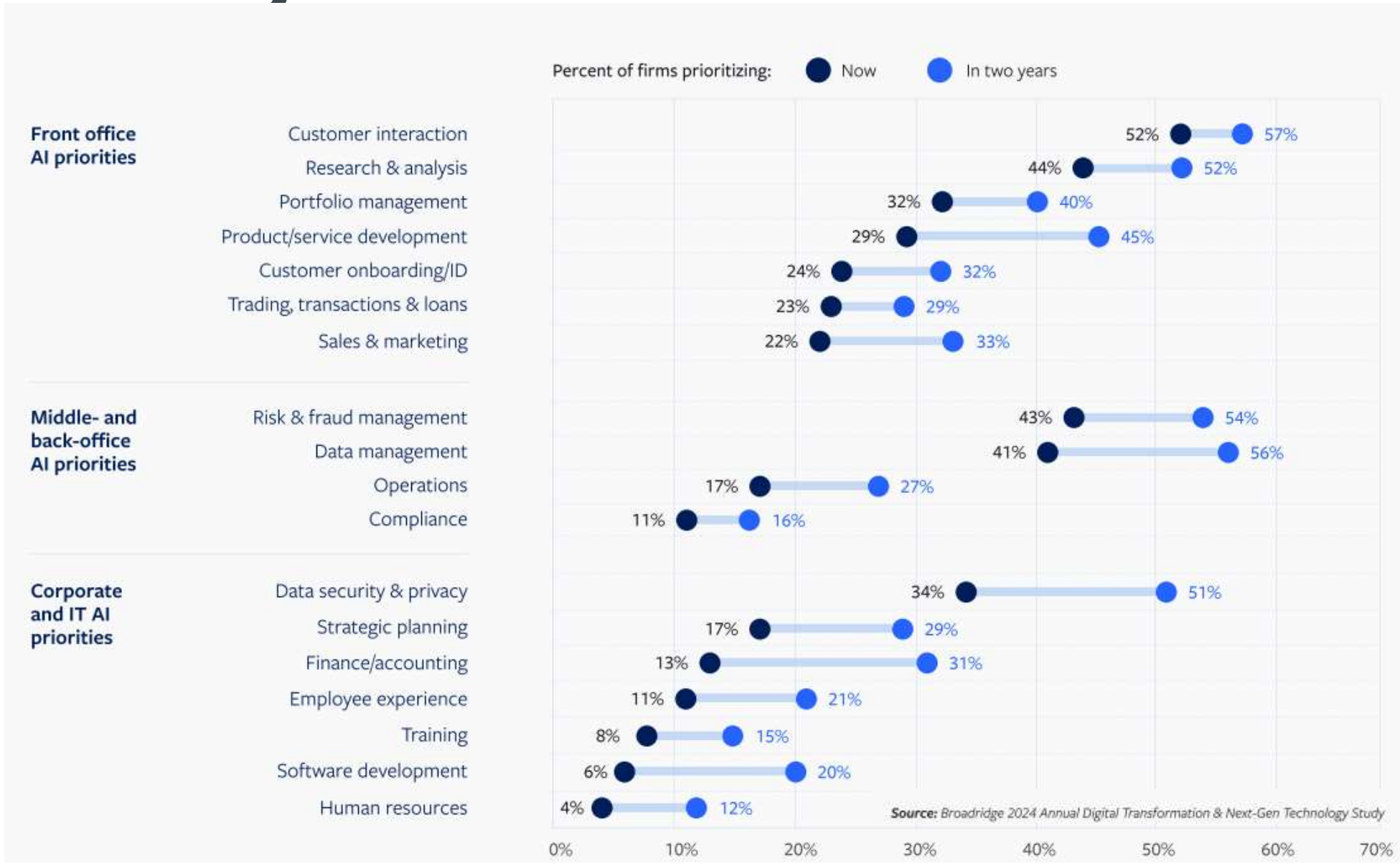
AUTOMATE COMPLIANCE

- streamline processes
- transaction monitoring and reporting
- fraud detection
- flag anomalies
- improving efficiency

Priority areas for AI

"More than 95% of firms surveyed are investing in AI, with top investment priorities in client-facing front-office functions such as customer interaction and research, as well as the data management systems to support those activities and the risk, fraud, and data security to protect them."

Broadridge 2024 Annual Digital; Transformation & Next-Gen Technology Study



mccarthy tetrault

Current Regulatory Approach Toward AI

Ontario Securities Commission

> *“AI systems can streamline complex tasks, optimize processes and uncover hidden insights and trends, all while learning and refining their capabilities. At the same time, the disruptive nature of AI systems has raised important questions about the role of regulation and governance in managing risks as well as the potential for its malicious use.”*
>
> Artificial Intelligence in Capital Markets – Exploring Use Cases in Ontario, September 2023

mccarthy tetrault

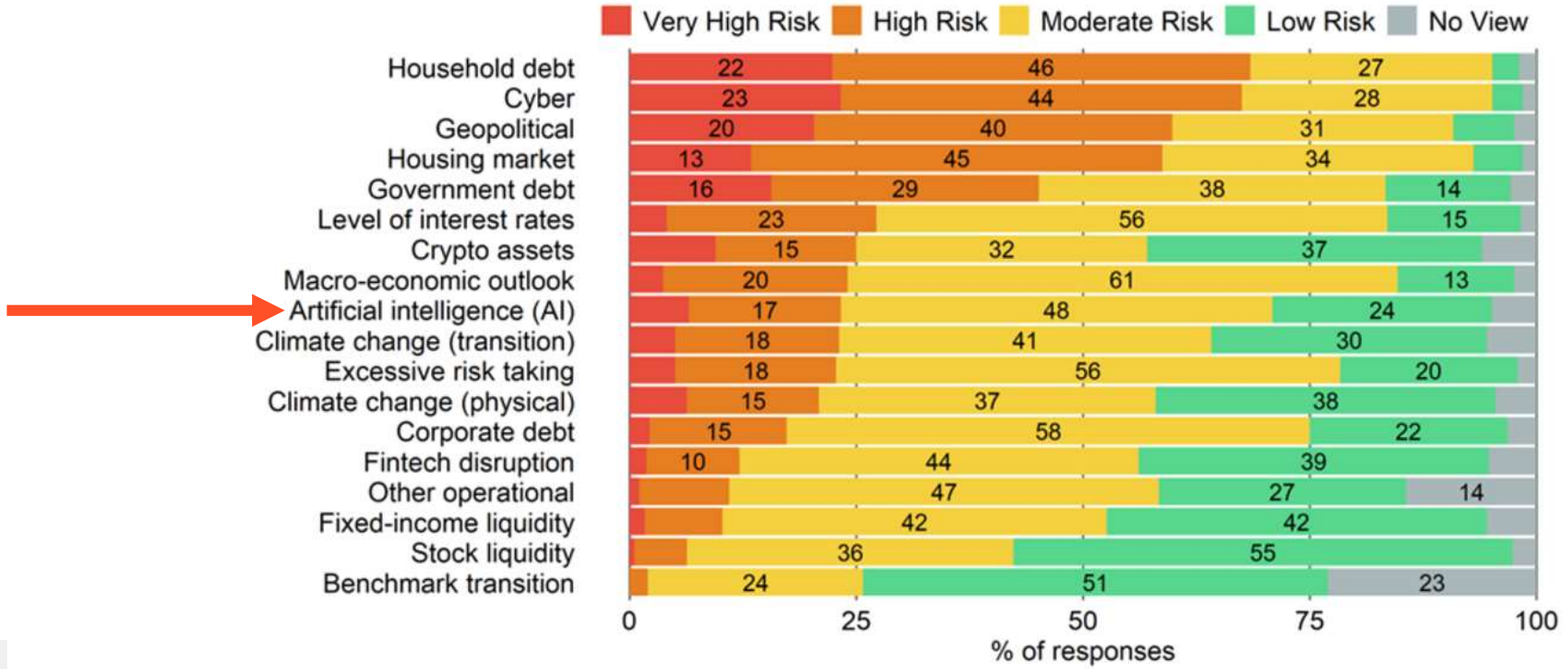
Regulatory Approach to AI: Where are we now?

- White Papers and Use Case Studies
- Public Statements and Guidance
- Consultation with Industry
- New Regulation
- Compliance Review & Inspection
- Individual Accountability
- Enforcement Actions
- Fines and Penalties

CSA's Systemic Risk Survey (2024)

> *"Respondents considered the risks associated with artificial intelligence (AI) to be moderate. Less than 25% of respondents thought AI poses a High Risk or Very High Risk to the financial system." CSA's* Systemic Risk Survey (2024)

Figure 3: Rate the following risks according to their potential impact on the stability of the Canadian financial system (2024)



Taking into account both the likelihood and severity of impact over the next 3 years.
Number of observations: 536 (2024). Source: CSA Systemic Risk Committee.

Regulatory view of AI

No Specific Rules. Yet.

— The OSC has acknowledged AI as a growing part of the investment industry

> *"If responsibly implemented, these applications have the potential to benefit retail investors. For example, they could reduce the cost of personalized advice and portfolio management. However, the use of AI within the retail investing space also brings new risks and uncertainties, including systemic implications"*
>
> "*[T]raditional governance approaches are insufficient in addressing [the] unique risks [of AI], such as lack of transparency, heavy reliance on different types of data, quality of data and bias in model selection*"

— AI is high priority in the OSC's Statement of Priorities for 2025-2026

— OSC recently released a report in October, 2023 titled "Artificial Intelligence in Capital Markets: Exploring Use Cases in Ontario" which explores various AI use cases in the investment industry followed by a companion report in September, 2024 titled "Artificial Intelligence and Retail Investing: Use Cases and Experimental Research"

— Likewise, CIRO released a study titled "Enabling the Evolution of Advice in Canada" that found an increased interest by compliance executives to adopt AI "capabilities over the next three years"

Human in the Loop Principle

Policy issues: costs vs. benefits / will innovation be stifled?

— For the OSC, the risks associated with AI have "reinforce[d] the need for a regulatory framework that ensures that the outputs of AI models are accurate and appropriate for retail investors."

— OSC has cited CSA Staff Notice 31-342 - *Guidance for Portfolio Managers Regarding Online Advice* (Staff Notice 31-342), issued in 2015 in response to the rise of robo-advisors), which provided regulatory guidance that investment decisions generated by algorithms must be overseen by humans

— This **"human in the loop"** principle is prevalent in discussions regarding regulatory frameworks for AI in various contexts. We expect that any CSA guidance issued in relation to AI will reinforce the requirements for some human oversight

— Registrants should also be guided by their core duties owed to clients when considering how to incorporate AI use cases into the portfolio management processes

  — statutory duty of care

  — duty of loyalty applicable

  — resolve material conflicts in the best interests of the client

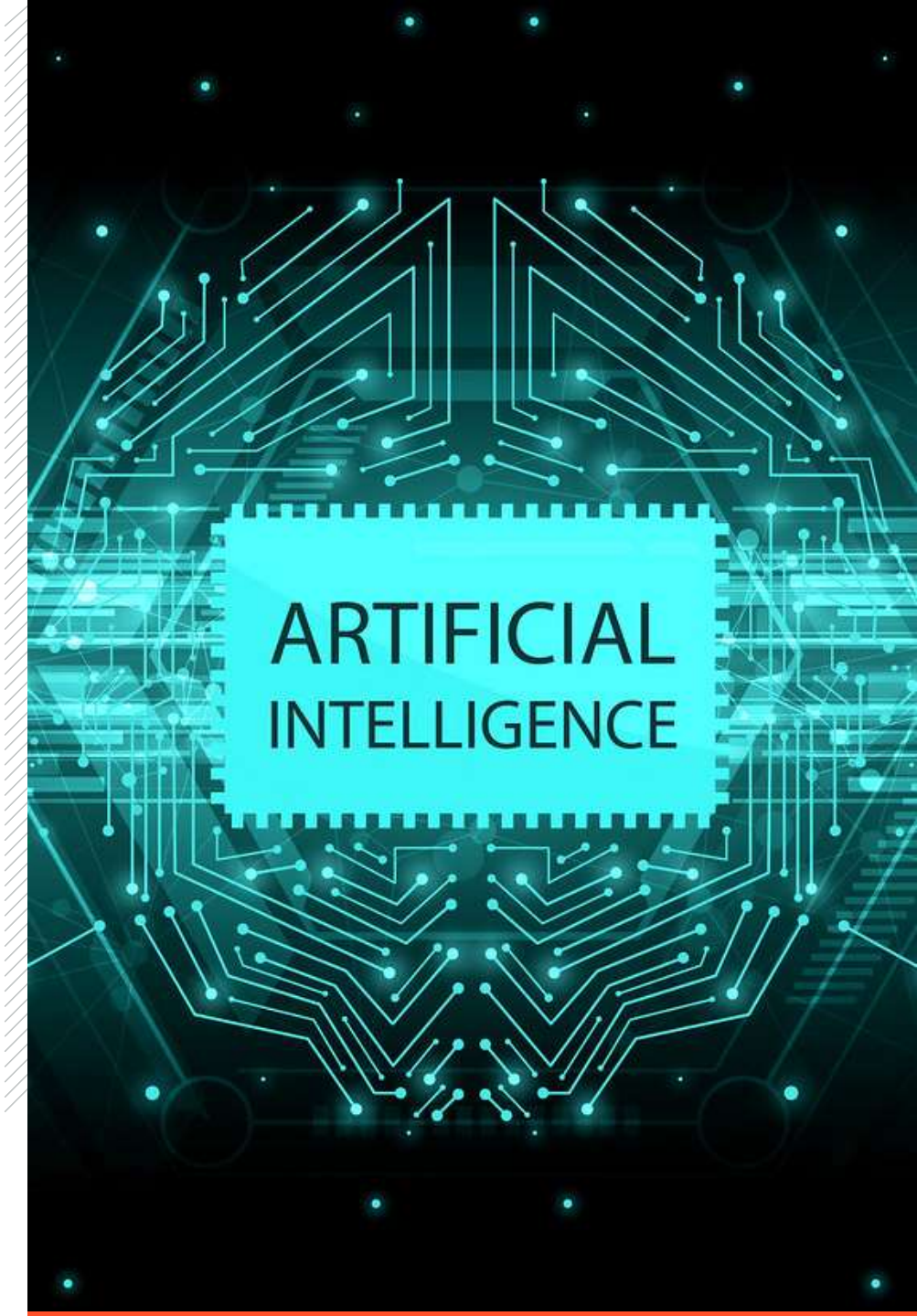
mccarthy tetrault

Future Regulatory Direction

mccarthy tetrault

How Are Securities Regulators Looking To Regulate AI?

- Transparency and Explainability
- Accountability and Governance
- Data Privacy and Protection
- Market Integrity and Fairness
- Compliance with Existing Regulations
- Testing and Validation
- Reporting and Disclosure
- Ethical use



mccarthy tetrault

AI Guidance Expected

> **"[T]here is a need to ensure that algorithms are based on high quality data, that factors contributing to bias are proactively addressed, and that these applications prioritize the best interests of investors rather than the firms who develop them."**

— OSC in their "Artificial Intelligence and Retail Investing: Use Cases and Experimental Research" report- September, 2024

mccarthy tetrault

US Approach to AI

Proposed Conflicts Rules

— SEC Chair Gary Gensler has commented that AI will cause a "nearly unavoidable" financial crisis without quick regulatory intervention, and their Division of Examinations has identified AI as a focus for 2024.

— The SEC proposed new rules to "eliminate, or neutralize the effect of, certain conflicts of interest associated with broker-dealers' or investment portfolio managers' interactions with investors through these firms' use of technologies that optimize for, predict, guide, forecast, or direct investment-related behaviors or outcomes."

— Some have criticized the proposed rules as overly broad, as their application would go far beyond AI and affect both individual and institutional investors. They have also been called too onerous, because they go beyond the "full and fair" disclosure regime typically seen in American securities law.

— Nevertheless, the OSC briefly referenced the SEC's proposed rules in its most recent report.

mccarthy tetrault

Litigation and Enforcement Risks, and How to Mitigate Them

mccarthy tetrault

AI Civil and Enforcement Risks From:

- Circumventing fiduciary duties via AI (i.e., too much delegation)
- Losing sight of the "human in the loop" principle in Staff Notice 31-342
  - How much oversight?
  - How much documentation (policies and procedures, testing, contingency plan(s), audit trail)?
- Alleged misrepresentations
  - Extent to which AI is used ("AI washing")
  - Extent of "human in the loop"
  - Risks from using AI

AI Civil and Enforcement Risks From: (contd.)

— Products that are alleged to be poorly designed

  — Predictive models will not always be accurate / unbiased

  — Will the firm be fully aware of how the technology has reached a certain conclusion?

  — What happens if AI uses corrupted, mislabeled or biased data?

AI Civil and Enforcement Risks From: (contd.)

— Material conflict of interest between use of AI and clients' interests

"*While the presence of conflicts of interest between firms and investors is not new, firms' increasing use of these [predictive data analytics]-like technologies in investor interactions may expose investors to unique risks. This includes the risk of conflicts remaining unidentified and therefore unaddressed or identified and unaddressed. The effects of such unaddressed conflicts may be pernicious, particularly as this technology can rapidly transmit or scale conflicted actions across a firm's investor base.*" **(SEC)**

AI Risk Mitigation – Remember Your Fiduciary Duties

Risk Mitigation Strategies

ESTABLISH POLICIES AND PROCEDURES, WITH CLEAR RESPONSIBILITIES AND ACCOUNTABILITY

To adequately oversee your AI tools, create written policies and procedures that ensure clear responsibilities, preparation for disruptions, etc.

DISCLOSE, AND ADEQUATELY ADDRESS, CONFLICTS

Conflicts should be disclosed and addressed in the best interests of the client, and considering the statutory duty of care and duty of loyalty applicable to portfolio managers.

KEEP A "HUMAN IN THE LOOP"

Staff Notice 31-342 requires at least some human oversight. For example, managers should "review the investor profile generated by the software to ensure it accurately reflects the information gathered in the KYC process," and ensure that model portfolios proposed by AI are suitable for the client.

ACCURATELY REPRESENT THE EXTENT TO WHICH YOU USE AI

Enforcement has been taken in the United States against companies engaging in "AI washing." When telling clients about the use of your AI, ensure your representations are accurate.

AI Risk Mitigation – Remember Your Fiduciary Duties

Risk Mitigation Strategies

CAREFULLY VET THE AI PRODUCTS YOU IMPLEMENT

Humans remain responsible for portfolio management. Complete extensive due diligence and ensure that the AI products you use are trustworthy.

ESTABLISH A CODE OF ETHICS (E.G., FOR CONFIDENTIAL INFORMATION)

Maintaining client confidentiality is crucial. Ensure that the AI tools you use have safeguards in place to adequately protect this information.

TRAIN EMPLOYEES TO USE AI PROPERLY

As part of having a “human in the loop” and maintaining human oversight, you should have training sessions on your AI tools to ensure that managers can sufficiently: (i) use AI to best serve their clients; and (ii) monitor the AI’s performance.

FREQUENTLY AUDIT YOUR AI TOOLS

Your AI policies and procedures should include a mechanism to periodically check important aspects of the AI tools you use. This may include data quality, security, trade execution statistics, benchmarking, and more.

Thank you.

Sean D. Sadler
ssadler@mccarthy.ca
416-601-7511

Shane C. D'Souza
sdsouza@mccarthy.ca
416-601-8196

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite MZ400
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

NEW YORK

55 West 46th Street, Suite 2804
New York NY 10036
UNITED STATES
Tel: 646-940-8970
Fax: 646-940-8972

LONDON

1 Angel Court, 18th Floor
London EC2R 7HJ
UNITED KINGDOM
Tel: +44 (0)20 7786 5700
Fax: +44 (0)20 7786 5702