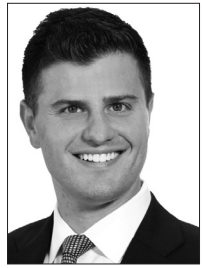
Data Protection and Cybersecurity in Canada

Andrae J. Marrocco, Lyndsay Wasser & Mitch Koczerginski

Mr. Marrocco

Ms. Wasser



Mr. Koczerginski

Maintaining robust data protection and cybersecurity protocols is critical to the development and reputation of international franchise systems. Data breaches disrupt business operations, devastate the goodwill and reputation of a franchise brand, and often result in an inordinate degree of legal liability.

Indeed, in most Canadian jurisdictions, businesses that suffer data breaches are subject to notification and reporting obligations, which include notifying impacted individuals in certain circumstances. To the extent the identity of individuals or their contact information are not known, businesses may need to provide indirect notification, which can include a public broadcast or publication.

Against the backdrop of ever-increasing Canadian data security regulation and scrutiny, it is imperative that international franchisors develop, implement, and effectively manage adequate policies and programs relating to the security of data to ensure that their franchise systems safeguard sensitive information in compliance with applicable legal and regulatory requirements.

Despite the need for better policies and programs, taking such steps involves an increased challenge for franchisors. The franchise business

Andrae J. Marrocco (Andrae.Marrocco@mcmillan.ca) is a Corporate/M&A partner and Co-Chair of the Franchise and Distribution Law Group in the Toronto office of McMillan LLP. He has particular expertise in complex franchise arrangements, franchise M&A, and cross-border/international transactions. Lyndsay Wasser (Lyndsay.Wasser@mcmillan.ca) is a partner in the Toronto office of McMillan LLP. Lyndsay focuses her practice in the areas of privacy, data protection, and employment and labour relations. Mitch Koczerginski (Mitch.Koczerginski@mcmillan.ca) is a litigation associate at McMillan LLP with a focus in franchise and distribution disputes. Mitch also has a strong background in privacy law and regularly advises and represents clients in connection with privacy and data breaches.

model, by virtue of its inherent structure is not only uniquely vulnerable to the harm caused by data breaches because of the independent entities operating and managing the ultimate customer facing businesses trading under the franchisor's brand, but also requires franchisors to work with their franchisees in implementing and maintaining the appropriate policies and procedures. Moreover, franchisors must foster a culture of data protection and cybersecurity awareness across the franchise system, map out the flow of customer information across the franchise network to identify any security gaps, understand and comply with the applicable legal requirements pertaining to personal information, and ensure that the respective rights and responsibilities of the franchisor and the franchisees are correctly reflected in the franchise agreement, the franchise disclosure document, and in actual practice.

This article provides a brief overview of the evolving Canadian legal landscape governing data protection and cybersecurity as it pertains to franchise systems with a particular focus on data breaches. The purpose of this overview is to familiarize the reader with sources of law that would affect organizational decision-making. More particularly, the article discusses the statutory framework of Canadian data protection laws (including cybersecurity) and the current state of the common law. Following the brief review of the legal landscape, we provide recommendations on how to minimize the risk of data security incidents to franchise systems, including developing, implementing, and maintaining a data security program with applicable policies and protocols.

It is worth pointing out that while Canada does have industry specific regulatory schemes that govern the processing of information in specific contexts (such as government, financial institutions, and healthcare providers), this article focuses on the general statutory scheme and common law that govern the security of customer's personal information in the Canadian private sector (i.e., outside of those industry-specific schemes).

I. The Statutory Framework Affecting Franchise Systems

A. *General Statutory Requirements*

In the Canadian private sector, a number of statutes regulate the manner in which businesses collect, use, disclose, store, and transfer personal information within their possession or control. The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[1] is of particular importance to franchisors. PIPEDA is the federal legislation that addresses the protection of personal information that is collected, used, and disclosed in the course of commercial activities (except where provinces or territories in Canada have

1. Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 [hereinafter PIPEDA].

enacted substantially similar legislation). PIPEDA is enforced by the Office of the Privacy Commissioner of Canada (OPC).

Currently, the provinces of Alberta,[2] British Columbia,[3] and Quebec[4] have enacted substantially similar legislation. Accordingly, this provincial legislation applies in place of PIPEDA within the relevant provinces and contains requirements that have been deemed to be "substantially similar" to PIPEDA. However, PIPEDA may continue to apply to businesses that transfer personal information from Alberta, British Columbia, and Quebec across provincial borders into a province or territory that is subject to PIPEDA.

PIPEDA contains a number of provisions pertaining to privacy and data protection. As stated above, the obligations apply to organizations engaged in commercial activities (which include both franchisors and franchisees) in respect of their handling of personal information.

More particularly, the obligations in PIPEDA respecting security safegurds include the following:

- Businesses are responsible for personal information under their control and must designate an individual or individuals who are accountable for compliance with the principles set out in Schedule 1 of PIPEDA.[5]
- Personal information must be protected by security safeguards that are appropriate to the sensitivity of the information.[6]
- Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, regardless of the format in which the information is held.[7]
- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.[8]
- The methods of protection should include (1) physical measures (e.g., locked filing cabinets and restricted access to offices); (2) organizational measures (e.g., security clearances and limiting access on a "need-to-know" basis); and (3) technological measures (e.g., the use of passwords and encryption).[9]

It is important to consider the flow of customer information—particularly personal information—across franchise systems in the context of the above requirements, including the type of personal information being collected

2. Personal Information Protection Act, SA 2003, c P-6.5 [hereinafter Alberta PIPA].
3. Personal Information Protection Act, SBC 2003, c 63 [hereinafter British Columbia PIPA].
4. An Act respecting the Protection of Personal Information in the Private Sector, CQLR c. P-39.1 [hereinafter Quebec Private Sector Act].
5. PIPEDA, sch. 1, art. 4.1.
6. *Id.* art. 4.7.
7. *Id*. art. 4.7.1.
8. *Id.* art. 4.7.2.
9. *Id*. art. 4.7.3.

and used, and which party makes use of the information. If franchise systems share customer personal information across the franchise network, whether between franchisees or between franchisees and the franchisor, or both, then comprehensive policies and procedures addressing that flow of personal information is critical. If the franchise system is less centralized, such that the personal information is being collected and used locally by each individual franchisee, then it is important to ensure that franchisees maintain policies and procedures to safeguard and prevent unauthorized access to such information. Franchisors should take the time to carefully consider the flow of personal information across their franchise systems, including how the responsibilities with respect to the protection of such personal information are divided between the franchisor and the franchisee. Moreover, it is critical to consider how those obligations will be documented in the franchise documentation.

B. *Statutory Requirements Relating to Data Breaches*

Regardless of whether customer information is shared across the franchise system or maintained solely by each franchisee, the reputational impact of data breaches will be felt across the entire network. When the public becomes aware of a data breach, even if the breach resulted from a failure of privacy safeguards of a single franchisee, the safeguards of the entire franchise system are often called into question by the public. Moreover, recent amendments to Canadian privacy laws have resulted in data security incidents being given increasing public attention.

For example, as of April 2019, the OPC reportedly has seen a four-to-five-time increase in the number of breaches reported to its office since the mandatory breach notification requirements came into effect in November 2018.[10]

Businesses that are governed by either PIPEDA or Alberta's private sector privacy legislation, the Personal Information Protection Act (Alberta PIPA), are currently required, in certain circumstances, to report data breaches involving personal information to the applicable privacy commissioner and notify the affected individuals.[11] While British Columbia and Quebec have not amended their respective private sector privacy legislation to contain such requirements, it is possible that they will follow suit to maintain their respective statuses as "substantially similar" to PIPEDA.

Under PIPEDA, a business that has suffered a breach may also be required to notify any government institutions or organizations that it believes can reduce or mitigate the risk of harm.[12] For example, this may

10. Jason Contant, *Early Numbers from Privacy Commissioners on Mandatory Breach Reporting*, Canadian Underwriter (Apr. 5, 2019), https://www.canadianunderwriter.ca/insurance/early-numbers-from-privacy-commissioners-on-mandatory-breach-reporting-1004161652.

11. *See* PIPEDA § 10.1; Alberta PIPA §§ 34.1, 37.1.

12. PIPEDA § 10.2(1)

include notifying a bank or payment processing service following a breach of payment information.

Failing to comply with the reporting requirements may also result in financial penalties. For instance, PIPEDA provides that it is an offence to knowingly contravene the reporting, notification, and record-keeping provisions described below. In the event of a failure to comply with the provisions, the Commissioner may refer the information to the Attorney General of Canada, who may then prosecute the business.[13] Knowingly failing to report to the OPC or failing to notify affected individuals when required to do so could attract a fine of up to $100,000.[14] Likewise, failure to notify the Office of the Information and Privacy Commissioner for Alberta (the Alberta OIPC) of a data breach affecting individuals in Alberta can also attract fines up to $100,000.[15]

Businesses should also consider that failing to notify individuals that their personal information has inadvertently been exposed as a result of a data breach may attract civil liability from such individuals, as addressed further below.

C. *When Reporting and Notification Are Necessary*

PIPEDA requires businesses to report and send notice of any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.[16] To trigger the reporting and notice requirement, a business must first determine whether a "breach of security safeguards" has in fact occurred. A breach of security safeguards includes the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from (1) a breach of a business's security safeguards and/or (2) the business's failure to establish those safeguards.[17]

For reporting to be necessary, the breach must involve personal information under the control of the business.[18] Neither PIPEDA nor its regulations define "control." A guidance document released by the OPC notes that, though the existence of "control" will be determined on a case-by-case basis, a business will largely be responsible for reporting a breach that occurs with any third party processor to whom the business has transferred personal information.[19] Franchisors may accordingly wish to include provisions

13. *Id.* § 20(4)(a).
14. *Id.* § 28.
15. Alberta PIPA, *supra* note 2, § 59(2).
16. PIPEDA §§ 10.1(1), 10.1(3).
17. *Id.* § 2(1).
18. *Id.*§ 10.1(1).
19. Office of the Privacy Commissioner of Canada, What You Need to Know About Mandatory Reporting of Breaches of Security Safeguards (Oct. 29, 2018), https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810 [hereinafter What You Need to Know].

within the franchise agreement that govern processing of customer information in order to clarify who retains control of such information.

Finally, to invoke the reporting requirement, it must be reasonable to believe that the breach creates a "real risk of significant harm" to an individual.[20] The number of individuals impacted does not matter.[21] As long as there is a real risk of significant harm to even one individual, the business is obliged to report the breach.

PIPEDA defines "significant harm" to broadly include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record, and damage to or loss of property.[22] In assessing whether a "real risk" of significant harm exists, the business must consider:

(a) the sensitivity of the information, including the context or circumstances of the breach;

(b) the probability that the personal information has been, is being, or will be misused, including factors such as how long and to whom the information was exposed, whether there was malicious intent behind the breach (such as theft or hacking), whether the information was adequately encrypted or anonymized, and whether harm has actually materialized; and

(c) any other factors prescribed in regulations enacted under PIPEDA.[23]

Moreover, a business must report a breach as soon as feasible after it determines that a breach has occurred, even if some information with respect to the breach is still unknown.[24]

D. *Content of the Report to the Commissioner*

The report to the OPC under PIPEDA must include the following information:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- the number of individuals affected by the breach or, if unknown, the approximate number;
- a description of the steps that the business has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;

20. PIPEDA § 10.1(1).
21. What You Need to Know, *supra* note 19, pt. 6.
22. PIPEDA § 10.1(7).
23. *Id.* § 10.1(8).
24. *Id.* § 10.1(6).

- a description of the steps that the business has taken or intends to take to notify affected individuals of the breach; and
- the name and contact information of a person who can answer, on behalf of the business, the OPC's questions about the breach.[25]

The report to the Alberta OIPC under Alberta PIPA must include the following information:

- a description of the circumstances of the loss or unauthorized access or disclosure;
- the date on which or time period during which the loss or unauthorized access or disclosure occurred;
- a description of the personal information involved in the loss or unauthorized access or disclosure;
- an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;
- an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;
- a description of any steps the business has taken to reduce the risk of harm to individuals;
- a description of any steps the business has taken to notify individuals of the loss or unauthorized access or disclosure; and
- the name of and contact information for a person who can answer, on behalf of the business, the Alberta OIPC's questions about the loss or unauthorized access or disclosure.[26]

Given that the breach reporting must be completed as soon as feasible and potentially before all details of the breach are known, franchisors should proactively work with franchisees to establish procedures regarding breach investigation and reporting.

E. *Content of the Notice to Individuals*

In addition to reporting the breach to the OPC, businesses governed by PIPEDA must also notify affected individuals.[27] The notification must include enough information to allow the individual to understand the significance of the breach of security safeguards to them and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or mitigate the harm.[28] It must also occur as soon as feasible after the business has determined that a breach of security safeguards involving a real risk of

25. Breach of Security Safeguards Regulations, SOR/2018-64 § 2(1) [PIPEDA Breach Reporting Regulations].

26. Personal Information Protection Act Regulation, Alta Reg 366/2003 § 19 [hereinafter Alberta PIPA Regulations].

27. PIPEDA § 10.1(3).

28. What You Need to Know, *supra* note 19, pt. 4.

significant harm has occurred.[29] Notifications must be conspicuous, non-legalistic, and easy to understand.

In particular, the notification must include the following information:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the business has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- contact information that the affected individual can use to obtain further information about the breach.[30]

Under Alberta PIPA, notification to individuals is required only if the Alberta OIPC, upon reviewing the breach report, requires the business to provide such notice.[31] If such notice is required, it must include the following information:

- a description of the circumstances of the loss or unauthorized access or disclosure;
- the date on which or time period during which the loss or unauthorized access or disclosure occurred;
- a description of the personal information involved in the loss or unauthorized access or disclosure;
- a description of any steps the business has taken to reduce the risk of harm; and
- contact information for a person who can answer, on behalf of the business, questions about the loss or unauthorized access or disclosure.[32]

Where notice to individuals is required to be given under applicable privacy legislation, it is generally required, with certain exceptions, to be given to individuals directly.[33] The delivery of notice has the potential to be costly for businesses depending on the number of individuals who must receive the notice and the manner of delivery.

29. PIPEDA § 10.1(6).
30. PIPEDA Breach Reporting Regulations, *supra* note 25, § 3.
31. Alberta PIPA, *supra* note 2, § 37.1(1).
32. Alberta PIPA Regulations, *supra* note 26, § 19.1(1).
33. PIPEDA § 10.1(5); Alberta PIPA Regulations, *supra* note 26, § 19.1(1)(a).

F. *Record Keeping Requirement*

Businesses governed by PIPEDA must also keep and maintain (for a period of at least two (2) years) records of all breaches of security safeguards involving personal information under their control, whether or not there is a real risk of significant harm.[34] Such records must contain sufficient details for the OPC to assess whether the business has correctly applied the real risk of significant harm standard and otherwise satisfied its obligations to report to the OPC and notify affected individuals.[35] To this end, businesses may wish to include a note in their records indicating why a breach of security safeguards did not trigger the obligation to report or notify (while being careful not to include any privileged legal advice).

Guidance released by the OPC provides that, at minimum, records must include:

- the date or estimated date of the breach;
- a general description of the circumstances of the breach;
- the nature of the information involved in the breach; and
- whether or not the breach was reported to the OPC and/or whether affected individuals were notified.[36]

Alberta PIPA does not contain a similar record-keeping requirement.

Looking at the above obligations, including the reporting and record keeping requirements, from the perspective of the franchise business model and, more particularly, from the perspective of the franchise arrangement and documentation, franchisors must (1) analyse the flow of personal information and determine who is primarily responsible for compliance with statutory obligations in all conceivable circumstances (as there may be different scenarios under which the franchisee will be primarily responsible for reporting an incident in some situations, and others in which the franchisor will be responsible); (2) carefully consider and implement policies, protocols and procedures to ensure that franchisees comply with, and assist the franchisor in complying with, the statutory obligations; and (3) ensure that the respective obligations (in the various scenarios considered) are reflected in all franchise documentation including the franchise agreement and operations manuals. Clearly, the above recommendations must take into account how personal information is specifically handled by the franchise system, and whether the franchisor wants to (and is permitted to) take control of the compliance obligations.

34. PIPEDA § 10.3(1).
35. PIPEDA Breach Reporting Regulations, *supra* note 25, § 6(2).
36. What You Need to Know, *supra* 19.

II. The Common Law

In addition to the statutory framework described above, an evolving body of Canadian case law is developing in response to individual and class action claims related to data breaches.

While there have already been many data security class actions in Canada, it is widely expected that such actions will become more frequent because of the mandatory notification obligations. Moreover, Canadian courts are becoming increasingly amenable to finding liability for breaches of privacy.

For example, in January 2012, the Ontario Court of Appeal recognized a new tort of "intrusion upon seclusion," whereby:

> One who intentionally [or recklessly] intrudes, physically or otherwise, upon the seclusion of another or his [or her] private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.[37]

The court found that a central rationale for recognizing this new cause of action was the unprecedented power of businesses to capture and store vast amounts of personal information using modern technology.[38] Highly sensitive personal information is accessible and collated with relative ease, including financial and health information, as well as data related to individuals' location, communications, shopping habits, personal interests, and more. The court found that the common law needs to evolve to reflect the modern technological environment.[39]

In February 2016, the Ontario Superior Court recognized another privacy-related tort in *Jane Doe 464533 v ND*[40] whereby:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[41]

In recognizing this tort, the court again acknowledged that the current state of technology enables predators and bullies to victimize individuals on a much larger scale than in the past, that society is scrambling to catch up to the problem, and that the law is only beginning to respond.[42] Given the judicial commentary in these two relatively recent cases, in absence of the enactment of new privacy legislation, or the amendment to current privacy legislation, a real possibility exists that additional torts may be recognized by Canadian courts in the future to respond to particular fact patterns involving privacy breaches. Of course, claims involving data breaches are also founded in more traditional causes of action, such as negligence, breach of contract and statutory breach (e.g., breach of consumer protection legislation).

37. Jones v. Tsige, 2012 ONCA 32, para. 19 (Can.).
38. *Id.* para. 67.
39. *Id.* para. 68.
40. Jane Doe 464533 v ND, 2016 ONSC 541 (Can.).
41. *Id.* para. 41.
42. *Id.* para. 16.

A trend that is beginning to emerge in Canadian data security lawsuits and, in particular, invasion of privacy lawsuits, is the division between:

(1) claims against defendants who are alleged to have committed the wrongdoing themselves (i.e., a company that has invaded the privacy of its own customers); and

(2) claims against companies who are alleged to have failed to protect information under their control from theft or unauthorized access by others (e.g., a company that has had its system breached by a third party).

While this article has identified the reputational risk associated with franchisor's misuse of customer data, the trend in lawsuits is more in line with the second type of claim, where plaintiffs sue alleging that the companies should have implemented further preventative safeguards. These latter claims expose franchisors to significant legal liability following breaches of data collected or held by their franchisees. There is a genuine basis for plaintiffs to allege that franchisors ought to have prescribed better safeguards, controls, and training programs with respect to the data collection and handling practices of their franchisees.

III. Class Action Litigation

Although individual lawsuits related to data protection and cybersecurity are possible in Canada, the bigger concern for most businesses is the rise in class action lawsuits. In Canada, these lawsuits tend to fall under two broad categories: (1) internal breaches and (2) external breaches by third party actors.

A. *Internal Breaches*

Canada has seen a number of class actions following intentional unauthorized access to or disclosure of personal information by the business's own employees, including:

- a class action following an employee of the Western Regional Integrated Health Authority allegedly accessing approximately 1,043 medical records without authorization;[43]
- a class action following allegations that employees of the Peterborough Regional Health Centre accessed patients' personal health information and distributed it to third parties without their consent;[44]
- a class action following a mortgage officer giving customers' confidential information to his girlfriend who then distributed it to persons who used it to commit identity theft and fraud;[45] and

43. Hynes v. W. Reg'l Integrated Health Auth., 2014 CanLII 67125.
44. Hopkins v. Kay, 2014 ONSC 321 (Can.).
45. Evans v. Bank of Nova Scotia, 2014 ONSC 2135 (Can.).

- a class action following a teacher and photographer of a ballet school allegedly taking sexually explicit photographs of students and selling them online without their knowledge or consent.[46]

The above is just a sampling of the class actions that have been filed following internal "snooping" or other unauthorized access and use of personal information by a business's own employees.

B. *External Data Breaches*

Class action lawsuits have also been filed following a number of data breaches caused by malicious external parties, including:

- a class action following data breaches affecting Target and Home Depot;[47]
- a class action following a high profile breach of the sensitive information collected by the Ashley Madison dating site;
- a class action following a data breach to Walmart's photo printing services website, which resulted in unauthorized access to personal and payment information of customers who had created an account;[48] and
- a class action following a breach of Casino Rama's employee, customer, and vendor data.[49]

Although many of these class actions are settled out of court, the plaintiffs' alleged causes of action include breach of contract, breach of consumer protection legislation, negligence, intrusion upon seclusion, breach of privacy, and publicity given to private life.

Notably, the Walmart litigation related to a breach of personal information under the control of one of Walmart's service providers. This case illustrates that, even where a breach of security safeguards occurs at a service provider level, it is possible that the business that hired the service provider may still be named in potentially expensive and embarrassing lawsuits.

IV. Reducing Legal Risk

Liability for insufficient or ineffective data security practices can arise in a number of ways. Breaches of the various statutes discussed earlier may result in complaints filed by groups or individuals, as well as audits or investigations initiated by the relevant privacy commissioner or other regulatory body. In addition, the regulators can publish a report of findings following an investigation, which may disclose the identity of businesses that are prosecuted or investigated, thereby harming those businesses' reputations.[50] Civil

46. Doucet v. Royal Winnipeg Ballet, 2018 ONSC 4008 (Can.).
47. Zuckerman c. Target Corp., 2015 QCCS 1285; Lozanski v. Home Depot Inc., CV-14-51262400CP (Ont. Sup. Ct.) (Can.).
48. Drew v Walmart Canada Inc., 2016 ONSC 8067 (Can.).
49. Kaplan v Casino Rama Services Inc., 2017 ONSC 2671 (Can.).
50. PIPEDA § 13(1); Alberta PIPA, *supra* note 2, § 38(1); Quebec Private Sector Act § 84.

disputes respecting cybersecurity issues may result in lengthy and expensive class action litigation, potentially large damage awards or settlement costs, and significant reputational harm.

To avoid these burdensome costs, franchisors should conduct an audit of their existing data security hygiene, including an evaluation of (1) who and what is connected to their systems and networks; (2) what software is running on their systems and networks; and (3) whether they have technology in place to prevent most breaches, rapidly detect breaches that do occur, and minimize the damage of such breaches (e.g., automatic shutdown when data leaks are detected). Businesses should also take into account the advice of privacy and data protection experts. For instance, the OPC, the Alberta OIPC and other provincial privacy regulators periodically release guidance on data security strategies and best practices.

Additionally, businesses should keep apprised of legislative changes to Canadian privacy law as it continues to evolve to meet the ever-increasing public call for stronger privacy protections. For instance, Innovation, Science and Economic Development Canada (ISED) recently released a "Strengthening Privacy for the Digital Age" discussion paper, which proposes amendments to PIPEDA as part of the federal government's Digital Charter initiative.[51] The Digital Charter outlines principles that Canadians can expect will guide the government's policy thinking and actions.[52]

The ISED's proposes to reform PIPEDA to (1) enhance individual control over their personal information and privacy; (2) enable responsible innovation in a manner that does not compromise privacy and security of personal information; (3) enhance the enforcement powers of the OPC in order to further incentivize compliance with PIPEDA; and (4) clarify PIPEDA to be more accessible and understandable to individuals and smaller organizations.[53] The ISED has encouraged stakeholders to contact it to assist it in developing the proposed legislative reform. Businesses should monitor legislative developments in order to keep apprised of any resulting changes to PIPEDA.

Notwithstanding the recommendations above, despite a business's best efforts, it is not possible to entirely eliminate the risk of a successful cyberattack. Therefore, franchisors may also consider insurance options to mitigate the risk of financial loss as a result of cyberattacks. Franchisors should contemplate whether their own policies will cover their franchisees or whether it is necessary to require franchisees to purchase their own insurance coverage as a term of the franchise agreement.

51. Gov't of Canada, Strengthening Privacy for the Digital Age (May 21, 2019), https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html [hereinafter Strengthening Privacy].

52. Gov't of Canada, Canada's Digital Charter: Trust in a Digital World (June 26, 2019), https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

53. Strengthening Privacy, *supra* note 52.

V. Conclusion

With data breaches regularly featured in news headlines, and class action lawsuits becoming alarmingly frequent, businesses would be well advised to consider the state of their data security hygiene and take steps to remedy any deficiencies.

As noted above, the franchise business model is uniquely vulnerable to data breaches because of the multiple independent entities operating and managing businesses under a single collective reputational umbrella. It is therefore critical that franchisors take the steps discussed in this article together with fostering a culture of data protection across the entire franchise system.

Data security is an area that requires a multidisciplinary approach, with input from a variety of experts. Therefore, a privacy audit will necessarily involve an evaluation of all relevant information technology systems, but must also include consideration of applicable legal and regulatory requirements. This step will often require an initial investment of time and resources, but franchisors that fail to actively address risks may be exposed to serious reputational, financial and legal repercussions if and when a data breach occurs.