National Banking Law Review

VOLUME 40, NUMBER 6 Cited as 40 Nat. B.L. Rev. DECEMBER 2021

• PRIVACY IMPLICATIONS OF AN OPEN BANKING SYSTEM IN CANADA •

By Darcy Ammerman, Mitch Koczerginski and Robbie Grant, McMillan LLP[1]

In August, Canada's Advisory Committee on Open Banking (the "**Committee**") released its final report (the "**Final Report**"), which provides the Committee's recommendations for how Canada should implement an open banking system. Since then, as part of their platform for reelection, the liberal government promised to move forward with a "made-in-Canada" open banking system that will launch no later than the beginning of 2023. Now that a liberal government has been reinstated, we anticipate ongoing development of Canada's open banking system.

This bulletin will focus primarily on the privacy and data security implications of an open banking rollout in Canada, and what related changes financial institutions and financial tech companies ("**fintechs**") ought to consider as the government installs the new framework. Please see our August 2021 bulletin[2] for an overview of the recommendations contained in the Final Report. You can also find general information about open banking in our previous bulletins on the topic from February[3] and July 2019[4].

• In This Issue •

LexisNexis®

WHAT IS OPEN BANKING?

Open banking is a regulatory framework that allows individuals and businesses to safely and securely share banking and transaction data with authorized third parties. By enabling the safe and secure access to information, open banking would allow fintechs to develop a new suite of useful financial services apps and products for the benefit of individuals and businesses. These services could range from budget-tracking, to tax assistance, to alternative credit worthiness measurements or addiction management tools.

Some fintechs already access consumers' financial data through "screen scraping", a crude process which directly copies information available on a consumer's financial account. However, screen scraping presents a significant threat to consumer privacy, since it frequently requires the consumer to disclose their banking login credentials and password. Furthermore, it may leave consumers without recourse if their information is accessed without authorization or

NATIONAL BANKING LAW REVIEW

National Banking Law Review is published six times a year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-409-91076-7 (print) ISSN 0822-1081
ISBN 0-433-44684-6 (PDF)
ISBN 0-433-44389-8 (print & PDF)

Subscription rates: $590.00 per year (print or PDF)
$670.00 per year (print & PDF)

Publications Mail
Registration No. 180858

misused.[5] An open banking framework would facilitate a shift away from screen-scraping towards a system that offers more safeguards to consumers and enhanced competition within the financial sector.

PRIVACY AND OPEN BANKING

Since open banking is predicated on the free flow of information, privacy is key to an open banking system. In its February 2019 Review into the Merits of Open Banking[6], the Committee said "[t]he trust needed to allow the digital economy to flourish, and the social license that organizations will need from Canadians to innovate with their personal data, hinges on having an appropriate legal framework in place that puts at the forefront key privacy issues." In its January 2020 review of stakeholder submissions, the Committee observed that all stakeholders considered privacy to be a significant risk of open banking.[7] In its own submission to the Committee[8], the Office of the Privacy Commissioner of Canada ("**OPC**") called for several privacy reforms to support an open banking system.[9]

Many of those reforms are already making progress. Before the election was called, the government had introduced a substantive overhaul to Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), in the form of Bill C-11, which would have enacted the *Consumer Privacy Protection Act* ("**CPPA**") (we summarized the proposed changes in a previous bulletin[10]). Bill C-11 died on the order paper when the election was called, but since the liberal government has now returned to office, a new privacy law bill is expected to be forthcoming. There is added international pressure for privacy reforms too, as the EU reviews Canada's adequacy status under the General Data Protection Regulation ("**GDPR**")[11]. Maintaining such status is crucial as it permits data processed in accordance with the GDPR to be subsequently transferred from the EU to Canada without requiring additional data protection safeguards or authorization to transfer the data.

Meanwhile in Quebec, *An Act to modernize legislative provisions as regards the protection of personal information* ("**Bill 64**") received Royal

Assent on September 22, 2021. This Bill amends Quebec's *Act respecting the protection of personal information in the private sector* ("**Quebec's Private Sector Act**") to include a data portability right, increased fines for non-compliance, and enhanced requirements for breach notification, consent, and data protection, among other changes.

So what further developments might we see on the horizon as the Canadian government implements an open banking system? And how should prospective open banking participants respond?

DATA PORTABILITY

In its June 2019 report on open banking, the Standing Senate Committee on Banking, Trade and Commerce recommended modernizing PIPEDA to align it with global privacy standards. It wrote that these changes "must include a consumer data portability right."

In the context of open banking, data portability means a consumer's right to direct that their personal financial information be shared with another organization. While this sounds simple in theory, it presents challenges for the organization sharing the data (typically the financial institution). First, personal information owned by the consumer is often grouped together with information owned by the sharing organization. For example, financial institutions may create "derived data" by processing consumer information together with proprietary algorithms and analysis.[12] The Final Report takes the position that the financial institution should generally be able to exclude derived data from an open banking system. However, if such data is normally available to the consumer, the financial institution should have an obligation to justify an exclusion.[13]

The second and related challenge is that sharing organizations may store and process data in a variety of formats, but for data portability to be meaningful, the personal information must be shared in a usable technological form. The difference between a string of loose data, and a properly organized spreadsheet is significant to the utility of such information for a third party app developer. Financial institutions can look to Quebec's Bill 64 as an example of how the concept of data portability could play out in practice. When it comes into force, Bill 64 will amend Quebec's Private Sector Act to provide consumers with a right to request their computerized personal information in a "structured, commonly used technological format" unless doing so raises serious practical difficulties.[14]

The introduction of a data portability right may require financial institutions to overhaul their data processing systems to ensure consumer data can be shared in a commonly used form, while separating out data that is unnecessary or proprietary to the financial institution. Depending on the sharing organization's data processing systems, data portability may require significant lead time to implement. The challenges outlined above are likely why the technological format amendment to Quebec's Private Sector Act does not come into force until September 22, 2024 (a full year after the majority of the amendments).

DATA SECURITY

From a technical standpoint, open banking requires financial institutions to make their application programming interface ("**API**") freely available to accredited, authorized third parties. This increased level of connectivity naturally comes with increased risk of fraud, financial crime and/or data breaches.

Furthermore, PIPEDA requires organizations to implement security safeguards commensurate to the sensitivity of the information,[15] and financial information has been recognized as "extremely sensitive" by the OPC and the Supreme Court of Canada.[16] Accordingly, open banking participants should expect strict data protection requirements to be introduced as part of an open banking framework.

The Final Report called for minimum data security measures for all open banking participants, including authentication, authorization, encryption, and audit trails. On the operational side, the Final Report also called for enhanced IT security infrastructure, incident response monitoring, and penetration testing, among other measures.

While established financial institutions should be familiar with many if not all of these protective measures, these requirements may be cumbersome for smaller fintechs looking to become accredited and enter the system. Companies looking to utilize open banking to develop new fintech solutions should keep these data protections in mind early on in their development.

LIABILITY

One important question in developing an open banking framework is which party is liable if financial data is accessed or disclosed without authorization. In its Final Report, the Committee suggested a simple concept that liability should "flow with the data" and rest with the party at fault. The Final Report called for a liability structure to prioritize consumer protection and redress, by requiring that the financial institution or third party service provider (as the case may be) pay out to the consumer immediately following their financial loss, and then work in collaboration with the corresponding party, or through alternative dispute resolution as needed, to seek compensation.[17]

The Final Report recommended that liability be aligned with provincial privacy legislation and guidance. Accordingly, open banking participants may wish to familiarize themselves with how Canadian privacy laws treat liability for breaches by organizations' service providers.

CONSENT

In its Final Report, the Committee called for specific rules around obtaining consumer consent. These include:

- a requirement for clear, simple and not misleading language;
- explanations of basic information such as what data is required, why such data is required, for how long it will be used, and possible risks of sharing that data;
- standardized consent processes; and
- a robust consent management system, such as a consent management dashboard.

These concepts are in keeping with current federal privacy legislation and guidance. When an organization collects sensitive information, PIPEDA generally requires express consent to be obtained,[18] and the OPC's guidelines on obtaining meaningful consent[19] already require the same information noted above to be brought to consumers' attention in a clear, simple manner. Furthermore, organizations processing sensitive customer personal information are already required under applicable privacy laws to manage and record consent.

TRANSPARENCY AND AUTOMATED DECISION MAKING

Since consumer trust is seen as fundamental to the success of an open banking system, transparency is a constant theme in the Final Report.[20] The Final Report calls for transparency in governance,[21] the accreditation process,[22] and the liability structure (including the complaint process and rules for compensation when something goes wrong). As the Committee wrote, "[t]he rules should be clear, simple and enforceable so that all consumers, at all levels of financial literacy and vulnerability to cybersecurity threats, can clearly see they are protected while using the system."[23]

One open question is whether further transparency requirements will apply to automated decision making, and the use of algorithms. In its own submission to the Committee, the OPC called for more attention to be paid to the use of big data analytics and artificial intelligence by fintechs. The OPC noted that the lack of transparency in the manner in which automated algorithms are employed in an open banking model can pose difficulties for individuals wishing to access their information and challenge compliance.[24]

On the one hand, automated algorithms are typically proprietary, and may not be subject to open banking regulation. However, there is an idea developing in privacy law that consumers have a right to know about automated decisions that

impact them. For example, Bill 64 will create a provision in Quebec's Private Sector Act requiring enterprises who make decisions based exclusively on automated processing of personal information to inform the person concerned of, among other things, the reasons and principal factors and parameters that led to the decision.[25] The proposed CPPA, before it died on the order paper, also contained a provision requiring organizations to make available a general account of their use of automated decision systems to make predictions, recommendations or decisions about individuals that could have significant impacts on them. The possible development of these rules is particularly relevant for automated investment management companies or similar third party robo-advisors.

REGULATORY POWERS OF ENFORCEMENT

In its submissions to the Committee in February 2019, the OPC called for increased enforcement powers for itself, including the ability to make orders, impose fines, and conduct audits without grounds in order to keep organizations accountable.

Quebec's Bill 64 will provide the Quebec *Commission d'accès à l'information* ("**CAI**") with the authority to levy large fines of up to $10 million in penalties or an amount corresponding to 2% of the company's worldwide turnover, whichever is greater. The proposed CPPA also authorized fines up to the greater of $10 million or 3% of the organization's gross global revenue, as well as providing the OPC with the power to issue "Compliance Orders". If the federal government tables similar legislation to the CPPA, it is anticipated that it will include similar penalties and enforcement powers.

CONCLUSION

Though federal privacy law now staggers behind Quebec, many indicators point to a significant reform on the horizon, in part due to developments relating to open banking. Financial institutions and third party fintechs should carefully monitor forthcoming privacy law developments, especially if they intend to participate in the open banking system in Canada.

If you have any questions about how to prepare for the regulatory changes relating to open banking in Canada, contact a member of our financial services group, or our privacy and data security group.

[***Darcy Ammerman*** *is an accomplished partner in McMillan LLP's financial services group with a focus on complex domestic and cross-border debt financing, financial institution regulation and "near insurance" such as extended warranties. Darcy frequently acts as Canadian counsel on cross-border lending transactions. Her transactional expertise includes syndicated lending, asset-based lending, DIP financing, high yield, subordinated debt, mezzanine financing and project finance/ PPPs. In the insurance area, Darcy advises on regulatory approvals, reorganizations and ongoing compliance matters. Darcy is a regular speaker on the topic of secured lending (including as part of the Osgoode Hall Intensive Short Course in Secured Lending & Debt Finance) and financial institution regulation, and known for her consistent substantive contributions to key industry publications. She is recognized in the IFLR1000 Financial and Corporate Guide, the Legal500 and as a Leading Practitioner in the 2021 Canadian Legal Lexpert Directory.*

Mitch Koczerginski *is a Canadian lawyer with a practice focused on retail and privacy issues. With a strong background in privacy law, Mitch advises and represents clients in connection with privacy and data breaches involving payment card information, personal information, health information and sensitive business information. Mitch routinely drafts and reviews privacy policies, conducts privacy and cybersecurity impact assessments and responds to access to information requests. Mitch also handles submissions to provincial privacy regulators as well as the Privacy Commissioner of Canada on a variety of matters, including breach reporting and access to information appeals.*

Robbie Grant *is building a practice in the regulatory group at McMillan LLP, with a focus on*

privacy and data protection. He frequently assists in drafting and reviewing privacy policies, responding to data breaches, and advising on the privacy law dimension of business practices and transactions. He also advises on interactions with privacy regulators, access to information requests, and privacy law considerations related to COVID-19. He is currently developing expertise in Canada's anti-spam legislation.]

---

1 Anthony Pallotta, formerly a financial services lawyer with McMillan LLP, also contributed to this article. He is now Legal Counsel (Financial Solutions) with Shopify Inc.

2 See https://mcmillan.ca/insights/open-banking-in-canada-could-2023-be-the-year/

3 See https://mcmillan.ca/insights/open-for-business-an-overview-of-open-banking-in-canada/

4 See https://mcmillan.ca/insights/a-call-to-action-on-open-banking/

5 *Final Report*, part 12 s.v. "Screen Scraping".

6 See https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html

7 Consumer-directed finance: the future of financial services.

8 See https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_fc_190211/

9 Office of the Privacy Commissioner of Canada, *A Review into the Merits of Open Banking: Submission to the Department of Finance Canada*.

10 See https://mcmillan.ca/insights/another-leap-forward-for-canadian-privacy-laws/

11 See https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210813/

12 *Final Report*, part 5.4.

13 *Final Report*, part 5.4.

14 *Bill 64*, section 112.

15 *PIPEDA*, Principle 4.7.

16 *Royal Bank of Canada v. Trang*, 2016 SCC 50, at para 36.

17 *Final Report*, part 7.1.

18 *PIPEDA*, Principle 4.3.6.

19 See https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

20 *Final Report*, part 1.

21 *Final Report*, part 6.

22 *Final Report*, part 8.

23 *Final Report*, part 7.1.

24 Office of the Privacy Commissioner of Canada, *A Review into the Merits of Open Banking: Submission to the Department of Finance Canada*, para 14.

25 Bill 64, section 102.

• IMPORTANT NEW DEVELOPMENTS APPLICABLE TO U.S AND OTHER FOREIGN BANKS OPERATING IN CANADA •

By Blair Keefe, Brigitte Goulard and Eli Monas, Torys LLP

This article summarizes several important new developments applicable to U.S. and other foreign banks operating in Canada.

NEW CONSUMER FRAMEWORK

A new financial consumer protection framework (the "Framework") applicable to Canadian incorporated banks and U.S. and other foreign banks carrying on business in Canada through a branch ("AFBs") is set to come into force on June 30th, 2022. The Framework will consolidate and strengthen the existing consumer protection regime applicable to Canadian incorporated banks and AFBs operating in Canada and will reinforce the powers of Canada's financial consumer protection agency, the Financial Consumer Agency of Canada ("FCAC"). This article will focus on the applicability of the Framework to AFBs only.

A number of the new obligations introduced in the Framework will impact the operations of AFBs operating in Canada and we have summarized below the more pertinent changes. AFBs that might have historically paid very little attention to the consumer protection provisions of the Bank Act (Canada) (the "BA") will be required to comply with the Framework upon its coming into force.

Application to Business Customers

The existing consumer protection regime under the BA is largely disclosure-based and focuses on retail customers. However, the Framework will introduce new responsible business conduct provisions which will also apply to business customers of an AFB, including:

- a general prohibition (added to the existing restriction on tied selling) on imposing undue pressure on a customer for any reason or taking advantage of a customer;
- the obligation to obtain a customer's express consent to an agreement and to provide the customer with a copy of the agreement prior to providing the product or service to the customer;
- the obligation to disclose certain prescribed fees and penalties in an agreement; and
- providing a business customer with authorized credit of less than $1,000,000, fewer than 500 employees and annual revenues of less than $50,000,000, the right to cancel an agreement with the AFB within 14 business days after the day on which the agreement was entered into (if the agreement was entered into by mail or by telephone), or within 3 business days where the agreement is entered into any other manner.

Complaints management

AFBs will be expected to comply with the Framework's onerous complaint management requirements. This may be particularly challenging since the new legislation broadly defines "complaint" to mean any dissatisfaction—whether justified or not—expressed to an institution with respect to either a product or service or the manner in which the product or service is offered, sold or provided. The scope of this definition catches all products and services regardless of the nature of the customer and therefore will also apply to complaints made by business/wholesale customers. Under this complaint regime, AFBs will be required to:

- designate an employee or officer to implement complaint management procedures and an employee or officer to receive and deal with complaints;

- establish complaint procedures ensuring that the complaints can be addressed within 56 days of receipt;
- send the customer a written acknowledgement of the complaint;
- make a comprehensive record of each complaint, including information as to how the AFB attempted to resolve the complaint and any paid compensation;
- annually make certain information available on the AFB's website, such as the number and nature of complaints the AFB dealt with, the average length of time taken to address complaints, and the number of complaints that have been resolved to the satisfaction of customers; and
- submit quarterly reports of complaints to the Commissioner of the FCAC, in a form satisfactory to the Commissioner.

Whistleblower Requirements

The whistleblower regime imposed by the Framework will enable AFB employees who have reasonable ground to believe that the AFB, or any person, has committed or intends to commit a "wrongdoing" to report it to the AFB, regulators or law enforcement agencies. "Wrongdoing" is defined as including a contravention of (i) any provision of the BA or the regulations made thereunder, (ii) a voluntary code of conduct adopted by the AFB or a public commitment made by the AFB, and (iii) a policy or procedure established by the AFB. Policies and procedures will be required to be implemented for dealing with wrongdoing matters and AFBs will be prohibited from taking action against such employees (such as disciplining, harassing, suspending or demoting the employee).

Application to Third Parties

Under the existing BA, AFBs are required to ensure that third parties that sell or further the sale of an AFB's products comply with the BA's consumer provisions. However, given the Framework's broader scope (in particular, the new complaint management requirements), the accountability of AFBs vis-à-vis third parties will be much more onerous and will require AFBs to re-examine their third parties' compliance with the new requirements.

FCAC New Enforcement Powers

The penalties for AFBs found in violation of the Framework have increased from up to $500,000 to up to $10,000,000. The FCAC will also name any AFB that is issued a notice of violation and can require an AFB to reimburse customers when financial harm occurs.

OSFI GUIDELINE ON FOREIGN ENTITIES OPERATING IN CANADA ON A BRANCH BASIS

On June 28, 2021, the Office of the Superintendent of Financial Institutions ("OSFI") released the final version of its *Guideline E-4: Foreign Entities Operating in Canada on a Branch Basis* ("Guideline E-4"). Guideline E-4 sets out OSFI's expectations with respect to the responsibilities of foreign entities operating in Canada on a branch basis and their management in overseeing the day-to-day operation of their businesses in Canada.

Branch Management

OSFI expects that individuals, who are authorized and responsible for overseeing a foreign entity's business in Canada ("Branch Management"), are knowledgeable of all applicable Canadian legislation, regulation, and guidelines related to the foreign entity's federally regulated business in Canada. However, OSFI does not require any one individual to have all such knowledge, although it does expect the composition of Branch Management to be commensurate with the overall size and complexity of the foreign entity's federally regulated business in Canada.

Branch Management should be satisfied that the business plan and policies of the branch appropriately

comply with the relevant Canadian regulatory requirements and OSFI expects that Branch Management will oversee and implement:

- the foreign entity's business objectives, strategies and plans;
- risk management policies and procedures, and related risk management control;
- policies and procedures to manage the assets and liabilities recorded on the branch's books and related accounts; and
- an independent assessment of the adequacy and effectiveness of the risk management controls.

Record Keeping

OSFI expects records to be updated and accurate as at the end of each business day[1], and that the records will be sufficiently detailed to enable:

- OSFI to conduct an examination and inquiry into the business of the branch;
- OSFI to manage the branch's assets, prior to the appointment of a liquidator, should the Superintendent of Financial Institution Canada (the "Superintendent") take control of the branch's assets in Canada; and
- the liquidator to conduct an effective liquidation of the branch's assets in Canada.

Electronic records must be capable of being reproduced in intelligible written form within a reasonable period of time. OSFI expects electronic records to be accessible and intelligible without incurring additional costs and using readily available commercial applications. For certain types of information, such as reinsurance arrangements or files on more complex activities, reproduced electronic records may not be sufficient for OSFI's review and the executed copy may need to be available, upon OSFI's request.

OSFI expects AFBs to keep copies of their records at their principal office in Canada and expects foreign entities governed by the *Insurance Companies Act* (Canada) to keep their records at their chief agency in Canada. Records stored in an electronic format must be kept on servers that are physically located in Canada. However, as noted below, some foreign entity branches may be exempt from the requirements to maintain records in Canada. In those circumstances, the branch must provide OSFI with immediate, direct, complete and ongoing access to the records that are stored outside Canada.

RECORD KEEPING REQUIREMENTS

Historically, the BA provided that certain records (e.g., records showing, for each customer of the institution, on a daily basis, particulars of the transactions between the institution and that customer and the balance owing to or by the institution in respect of that customer) must be kept at the head office of the institution or such other place in Canada as the directors think fit.

Effective June 30, 2021, the BA (together with the *Trust and Loan Companies Act* (Canada) and the *Insurance Companies Act* (Canada)) was amended to provide that the record keeping requirements above do not apply to an institution that is a subsidiary of a "regulated foreign entity"[2] or, in the case of a bank, that is a subsidiary of a foreign bank incorporated or formed outside of Canada in which a trade agreement listed in a new Schedule IV of the BA is applicable.[3] However, where such an institution maintains those records outside Canada, the Superintendent may, in the case of "a", and must, in the case of "b", direct the institution by order to maintain a copy of those records at any place in Canada as the directors see fit:

a. if the Superintendent is of the opinion that he or she does not have immediate, direct, complete and on-going access to those records; and
b. if the Superintendent is advised by the Minister of Finance that the Minister is of the opinion that it is not in the national interest for the institution not to maintain a copy of those records at any place in Canada.

A new provision was also added to allow for regulations to be published respecting the records, papers and documents to be retained by an institution,

including the length of time those records, papers and documents are to be retained, and what constitutes immediate, direct, complete and ongoing access, for the purpose of paragraph "a" above.

If you would like to discuss any of the information in this article further, or have any additional questions, please reach out to the authors.

[***Blair Keefe*** *is co-head of the Torys' Financial Services, Bank Regulatory and Insurance Regulatory practices, and is co-head of the Payments and Cards Practice. His practice focuses on corporate and regulatory issues relating to financial institutions, including mergers and acquisitions and corporate finance.*

Brigitte Goulard *is co-head of Torys' Consumer Protection Practice and a former Deputy Commissioner of the FCAC. She has more than 25 years of experience working in the financial services sector, including the banking, insurance, and financial cooperative sector. Her practice focuses on consumer protection matters and regulatory issues relating to financial institutions and government-related matters.*

Eli Monas's *practice focuses on corporate law and regulatory issues relating to financial institutions. He has been involved in a number of significant transactions involving Canadian and foreign financial institutions. Eli also completed a six-month secondment to the Legislation and Approvals Division at the Office of the Superintendent of Financial Institutions in 2017-18.*]

---

1 Records that change less frequently than daily remain accurate until they change. Accordingly, records should be updated daily or at the frequency with which they change.

2 "Regulated foreign entity" means an entity that is: (a) incorporated or formed outside of Canada in which a trade agreement listed in Schedule IV of the BA is applicable; and (b) subject to financial services regulation in that country or territory.

3 Schedule IV of the BA includes the following trade agreements: (a) the Canada-Chile Free Trade Agreement; (b) the Canada-Peru Free Trade Agreement; (c) the Canada-Colombia Free Trade Agreement; (d) the Canada-Panama Economic Growth and Prosperity Agreement; (e) the Canada-Honduras Economic Growth and Prosperity Agreement; (f) the Canada-Korea Economic Growth and Prosperity Agreement; (g) the Canada-European Union Comprehensive Economic and Trade Agreement; (h) the Comprehensive and Progressive Agreement for Trans-Pacific Partnership Implementation Act; (i) the Canada-United States-Mexico Agreement; and (j) the Canada-United Kingdom Trade Continuity Agreement Implementation Act.