

Prof. Michael R. King
Co-Founder, Scotiabank Digital Banking Lab
Ivey Business School, Western University
1255 Western Road, London ON N6G 0N1
February 26, 2019

The Advisory Committee to the
Open Banking Review/Financial Institutions Division
The Financial Sector Policy Branch
Department of Finance Canada,
90 Elgin Street, Ottawa, ON K1A 0G5
fin.OBBO.fin@canada.ca

Dear Advisory Committee,

RE: Follow-up on Vancouver Consultations on Open Banking

Following our meetings in Vancouver on February 14, I wrote the attached article for the *Ivey Business Journal* that summarised some recommendations. The article is titled “Who Owns Your Banking Data?” and is available at: <https://iveybusinessjournal.com/who-owns-your-banking-data/>

I hope you find it useful.

Best,



Michael R. King

Who Owns Your Banking Data?

By Michael R. King, Associate Finance Professor, Ivey Business School.

Ivey Business Journal, January / February 2019

Canada's Department of Finance recently began cross-country consultations on open banking—a global trend enacted last year in the UK and European Union and soon rolling out in Australia.

Why should you care? Under open banking, you would be able to authorize apps developed by FinTech companies to access your bank account in order to provide services you want such as reporting, budgeting or forecasting. In other words, the debate is ultimately about who owns consumer banking data—you or your bank—and may set the regulatory framework that will guide discussions on data privacy, cybersecurity, and digital identity.

While you may think it foolish to share your banking data with a third-party, many Canadians who want a comprehensive picture of their finances are already doing it. The current process is painful. You download files onto your computer and try to make sense of it all. Or you give your banking password to a company that does the same thing using screen scraping technology – basically converting screen shots into data that can be analysed.

In my session, everyone agreed on the necessary steps to make open banking work for Canadians. The issues that need to be addressed are scope, security, stages, and literacy.

The scope of open banking can be narrow or broad. It may only cover your bank account and mortgage, or it can encompass your bill payments, investments, insurance and more. While open banking in the UK and EU included payments, it will not in Canada. Why? Canada's payment system is getting a major upgrade, so the plan is to leave it out until modernization is complete. But excluding payments will reduce a lot of useful functionality for consumers, and it should be phased-in later.

Data security (and privacy) is the #1 issue. This problem is not unique to open banking. It affects every aspect of our digital lives. Our smart phones, smart speakers, smart cars and smart household devices are storing and transmitting data. Any FinTech entrusted with access to our financial data will need to demonstrate the ability to transmit, store and protect our data. Eventually, Canada needs to establish both data protection standards and a code of consumer data rights to get the most out of the digital economy.

Canada's proposal does not include a digital identity system to replace physical documents (such as a passport or identity card). A digital identity is a set of electronic records that an individual controls and uses to complete transactions. India's national digital identity program, called Aadhaar, provides credentials to all of its citizens irrespective of income level, employment or abode. The UK, France, Netherlands, Denmark, Japan and Australia are all introducing some form of eID. In Canada, early efforts are underway but should be tied to open banking in the future.

Canada should adopt two standards to increase security. The safest way to transmit data is directly from one computer to another using application programming interfaces (APIs). An API is set of software protocols (or rules) that allow computers to talk to each other. Canada's open banking legislation needs to mandate standardized APIs that third-party developers can use to build banking apps for customers.

Another standard to adopt is the Payment Card Industry Data Security Standard (PCI DSS). It was adopted by the major credit card companies in 2004 to reduce credit card fraud and protect cardholder data. It specifies twelve requirements for building and maintaining a secure network. Any FinTech firms operating in payments must demonstrate they are PCI DSS-compliant. Open banking can build on this global standard, rather than starting from scratch.

Canada should roll-out open banking in stages. Doing too much too soon may create unexpected problems for the banks and confuse consumers. Initially the UK required only its largest nine banks to comply with open banking legislation. Australia is phasing-in credit and debit cards first, deposit and transaction accounts next, and mortgages last. Canada should follow a staged, predictable roll-out to enable bank compliance and consumer adoption.

Finally, open banking must be accompanied by a major effort to raise financial literacy. Consumers need to be informed and protected. Education will be most effective at the “point of use” when a consumer is about to authorize access. Educational videos should be available. Terms, conditions and risks should be explained in simple, clear language, not in end-user agreements full of legal jargon. Transparency around fees should also be required.

The consensus in my session was that Canada should legislate open banking sooner rather than later. Otherwise Canadian consumers and small businesses will be underserved and our banks and FinTech companies will not have the same incentive to innovate. A failure to adapt to this global trend would leave our financial sector at a disadvantage, stuck in a digital ice age.