WHITE PAPER

flinks

The State and Future of Financial Data Connectivity in Canada

How screen scraping is paving the way for open banking

Table of contents

flinks

Flinks is a data company that empowers businesses to connect their users with financial services they want.

Trusted by hundreds of world-class companies, Flinks enables businesses to connect users' bank accounts, enrich their data, and utilize it to deliver better products.

An award-winning company, Flinks has become the leader in financial data connectivity in Canada in just three years, and is well on its way to becoming a global leader.

Flinks.io

Key takeaways

Screen scraping currently serves a significant purpose in Canada.

It is hands down the most widespread technology employed to collect user-permissioned financial data. Screen scraping enables the transmission of a wide range of types of data, which in turn supports a growing number of innovative financial products. In essence, companies like Flinks already provide a data connectivity infrastructure, which currently powers hundreds of businesses servicing 3.5 to 4 million Canadians, over 15% of the adult population.

The fact that connectivity currently relies on screen scraping doesn't pose a particularly new or significant security risk – quite the opposite.

Credentials sharing has been happening for a long time with web browsers and password management apps, with risks being mitigated by effective information security programs. The real risk of delaying a formal open banking framework is allowing a patchwork of private, non-standard and non-transparent agreements between banks and aggregators to take place instead of a fully inclusive – and competitive – ecosystem.

Focusing on screen scraping is a waste of energy – and more importantly, a waste of time.

Ensuring a competitive environment in financial services requires mass adoption of data connectivity. This is a serious and urgent challenge: Canada risks falling behind if it doesn't implement an open banking framework. In this regard, screen scraping can and should be replaced by a more sophisticated technology. Both industry research and anecdotal evidence show that the replacement must be as good as the current method on numerous fronts.

Future financial data connectivity needs to expand on the current benefits of screen scraping as much as it needs to overcome its shortcomings.

Open banking is not defined by a specific technology, be it screen scraping or API.

Open banking is technology agnostic – it's about financial data connectivity and consumer empowerment. Businesses can and should start experimenting with financial data connectivity using a trusted aggregation provider. Starting now to learn how to use the new infrastructure of finance is what will allow them to build a competitive edge in an evermore crowded marketplace.

Introduction

Despite the current context, Canada is heading toward open banking. In the federal political apparatus, consultations have been launched at both the legislative and executive levels of government. Advisory firms are drafting up scenarios, the industry is bracing itself for the upcoming disruption, and innovators are already moving to seize new opportunities.

Open banking will modernize Canada's financial services sector with a digital infrastructure enabling consumers to easily transfer their bank data to third parties, thus paving the way for greater consumer choice in terms of financial services, a traditionally oligopolistic sector. The question is no longer if or when, but rather how will this happen; however, significant uncertainty still remains around what this formal open banking infrastructure will look like.

There's no commonly accepted framework or mission statement yet. There's not even a clear consensus on whether open banking should be "read-only", or if it should include both "read" and "write" functions. In other words: should open banking be limited to sharing financial data, or should it also allow third party providers to initiate money transfers?

The narrower details are even more unpredictable. From the technical standards of the technology that will be used to share financial information, to the governance framework that will apply to the players of the ecosystem, pretty much all of the nuts and bolts have to be figured out.

Meanwhile

Financial data connectivity – a core function of the open banking infrastructure – already exists in Canada using a technology known as "screen scraping."

While adoption is on the rise for both businesses and consumers, screen scraping has a history of raising security and privacy concerns in certain circles. As a result, many financial businesses are left wondering if they should start experimenting with financial data connectivity right now, or wait for the implementation of a formal open banking infrastructure.

This white paper examines the claims against screen scraping, and in doing so provides a more balanced account of this technology and the role it plays in Canada.

WHAT ARE THE REAL RISKS?

Lifting the veil on screen scraping

Over the past few years, open banking has been the subject of its fair share of op eds and news articles. Perhaps one of the most recurring features of this coverage is an inquiry into the risks posed by screen scraping.

Screen scraping refers to the automatic capture of information displayed in a browser. The practice is legal in both Canadian and US case law. In fact, this technology isn't new at all: search engines have been doing it since the dawn of the Internet. It used, among other things, to transfer information from legacy systems to modern databases, acting as a format converter that allows data to be consumable on the receiving end. In short, there is no short-term scenario in which screen scraping is going away.

In finance, screen scraping is performed in the context of permissionned financial data connectivity. This process has three components: authentication, data collection, and data transmission.

Critics of screen scraping have concerns over security, privacy and attribution of liability. We examine these concerns below in the context of how we handle them at Flinks.

How does financial data connectivity work?

Aggregation providers are embedded in a financial business' digital experience, and act as trusted intermediaries in an exchange whereby end users share their financial data with the business in order to access its services.

1- AUTHENTICATION	2- DATA COLLECTION	3- DATA TRANSMISSION
End users are asked to identify their financial institution, share their online credentials with the aggregation provider, and provide permission to access their financial data.	Upon receiving consenting consumers' credentials, aggregation providers run a script to log into their financial institutions' online platforms and automatically collect, or "scrape", the data therein.	Aggregation providers organize the data, and store it into encrypted databases. The end user's data can safely be sent to the financial app this end user wishes to use, through a secure API and as per the permissions granted by the individual.

Lifting the veil on screen scraping

“Screen scraping puts consumers at risk”

A consumer’s financial data should be regarded as highly sensitive information. It is critical that it doesn’t fall into the wrong hands, so it is understandable that screen scraping must face scrutiny. Any claim that it is inherently risky, however, is misleading.

Screen scraping can be a highly secure technology in the context of collecting and transmitting end user-permissioned data. In fact, the risks are not with screen scraping itself, which is nothing more than a data collection technique. They actually hinge on the aggregation provider’s security practices around data handling.

Flinks has been vocal and transparent about the stringent requirements for providing robust security and high reliability in the context of financial data connectivity.

Governance

- **Security and Privacy Committee.** A Security and Privacy Committee is critical to make sure security governance is a continuous process – not an event. It brings together all key stakeholders to assess risks and vulnerabilities, implement appropriate controls, and perform internal audits to make sure they are effective
- **Audits and tests.** Routine tests and independent audits ensure the effectiveness of security controls and protocols. Aggregation providers should maintain a SOC 2 Type II report.

Security

- **No meaningful access.** As a general principle, no employee or third-party vendor of an aggregation provider should be able to access end users’ information in any meaningful way – even when there is a legitimate purpose.
- **Segregation of duties and least privilege principle.** An aggregation provider’s employees must always be granted the absolute minimum level of access they need to perform their duties. Their tasks must be split into parts and assigned to different people, making sure no one is solely in control.

Data management

- **Distinct databases.** Every client needs its own private instance and secure database. Token-based authorization and other security measures ensure all client communication with the aggregation provider’s API are legitimate.
- **Encryption.** Data has to be encrypted in transit and at rest using the latest algorithms, such as AES-256. End users must be assigned unique encryption keys, on regular and automatic rotation.

Compliance & legal

- **Compliance and monitoring.** Wherever they are, aggregation providers must comply with the relevant applicable privacy laws. In Canada, this includes PIPEDA, Canada’s federal privacy and data protection law.

WHAT ARE THE REAL RISKS?

Lifting the veil on screen scraping

“Sharing their credentials puts consumers at risk and/or violates their privacy”

Credentials sharing has been happening for a long time with web browsers and password management apps. Consumers trust these providers to store all kinds of online credentials, including bank login credentials, without compromising or misusing them.

> *Again, the real risks hinge on any company’s security practices as a whole.*

To sharply limit the risk that end users’ credentials will be compromised, we treat them differently than the financial data we handle. Credentials are encrypted and never shared with our clients in any way, shape or form. In other words, end users’ credentials are in fact maintained confidential: even if end users share their credentials with Flinks, they are not accessible without the encryption key that no individual has access to.

Credentials-based authentication is sometimes casted as a risky method, and compared to “safer” token-based or multi-factor authentication.

The fact of the matter is that there will always be a level of risk, no matter the technology in place. Tokens and cellphones can be compromised, too. Ultimately, consumers should weigh credentials-based financial data connectivity from a “value-to-risk” perspective.

"When consumers share their credentials, they violate their financial institution's terms of service"

Major Canadian banks are, for the most part, opponents of credentials-based financial data connectivity. They used to forbid credential sharing in earlier versions of their online terms of service.

Nowadays, it's not uncommon for banks to use financial data connectivity, too. They will, for instance, ask for their clients' bank credentials with other financial institutions, so they can access those clients' financial information themselves. Once against credentials sharing, the Canadian Banking Association (CBA) changed its stance on the matter to reflect such practices. The CBA now sees sharing login information with another financial institution as an acceptable means to achieve a "legitimate purpose."

Banks have been updating their terms of service agreements in light of this new reality. What they did, though, is to transfer most (if not all) liability onto their customers. There is a growing body of research suggesting that terms of service agreements are used by businesses to create a context of "take it or leave it". Such a context forces customers to accept the terms, even if they don't fully understand or don't really agree with them.

How effective are terms of service?

Terms of service were developed as a way to help consumers make informed choices by disclosing important information. But research suggests that, in practice, terms of service fall short of this goal.

NYU professor Florencia Marotta-Wurgler has studied the extent to which potential software buyers actually access and engage with end user license agreements.

She has found "that only 1 in 1,000 consumers access the license agreement – which is almost no one – and that most of those who do access it read no more than a small portion."

The future of financial data connectivity

Open banking empowers Canadians

The Canadian financial sector has been largely lagging behind other verticals when it comes to delivering high quality digital experiences. Financial businesses operate in high compliance environments, designed to protect their customers and the economy as a whole. As a result, finance has received less pressure than other sectors from disruptive newcomers to digitally transform.

Yet, the competitive landscape is changing. In its 2019 report, the Senate's Committee on Banking, Trade and Commerce points out that Canada "risks falling behind" if it fails to implement a formal open banking system, as it would "become an importer of financial technology rather than an exporter."

The essence of open banking is the idea that consumers own their financial data and should have agency over it. Consequently, an open banking infrastructure would level the playing field and allow new entrant innovators to compete in building the next generation of data-driven financial products.

Contrary to some paradigms, open banking isn't defined by any specific technology, be it screen scraping or APIs. Quite the opposite: it's about financial data connectivity and consumer empowerment, which are ultimately technology agnostic.

Empowering Canadian means giving them the ability to direct their data to be shared with third parties of their choosing.

The state and future of financial data connectivity

There's documented evidence of the need for a financial data connectivity infrastructure in Canada. Aside from the government-mandated report that has charted the merits of open banking, the value proposition has already been market-validated. At present time, financial data aggregators like Flinks act as trusted intermediaries for hundreds of financial businesses together servicing 3.5 to 4 million Canadians. This represents over 15% of the adult population, and adoption is on the rise.

The future of financial data connectivity

Screen scraping is by far the most widespread technology used by aggregation providers to collect user-permissioned data. As aggregation providers mature their products, they are able to lower the technical challenges for financial businesses to integrate data connectivity. Data transfers are quick, secure and convenient for consumers.

Screen scraping allows providers to collect and therefore transmit a wide range of types of data. This, in turn, supports a growing number of innovative financial products that couldn't exist otherwise. Yet, the current state of our data connectivity infrastructure should only be seen as a temporary solution.

> *API-based connectivity needs to expand on the current benefits of screen scraping as much as it needs to overcome its shortcomings.*

The trajectory of open banking in the U.S. shows that the absence of a formal framework opens the door to a patchwork of private, non-standard, and non-transparent bilateral agreements between banks and aggregators.

A formal open banking system is the way forward to a fully inclusive financial ecosystem. On the technical side, there's little doubt that data connectivity will be handled by APIs provided by the banks. API-based connectivity is an effective way to actualize high quality standards and oversight across the ecosystem.

As Canada navigates the transition to a formal open banking system, we need to be thoughtful of the significant role that screen scraping plays right now. Both industry research and anecdotal evidence show that the technology replacing screen scraping must be at least as useful and convenient.

The future of financial data connectivity

How a formal open banking system supports consumers and financial businesses

Liability. Properly allocating liability across the ecosystem. This means defining who needs to perform which actions to make the consumer whole again in the event they would, through no fault of their own, suffer a loss.

Open and transparent standards. Making the whole process more reliable with a stable, modern technology infrastructure – likely to be APIs – to handle the authorization, data collection and transmission steps.

More granular control. Providing consumers more control over what types of data are accessed, for how long, and for which purpose.

What would diminish the benefits of a formal open banking system

Limiting the quality of the experience. Slow APIs and complex permissioning flows make the whole user experience unpleasant and confusing. Financial data connectivity needs to be convenient and intuitive.

Limiting the availability and format of financial data. Screen scraping allows for the collection of a wide range of types of data, which is critical to power a variety of use cases. A formal open banking system should provide at least the same depth and breadth of data.

Will financial aggregators still be relevant under open banking?

Even if banks provide their own APIs, most businesses won't dedicate the time and resources needed to build and maintain the connections to so many data sources. They will turn to a financial aggregator to handle those connections, and simply collect data coming from a single point of integration.

At Flinks we believe that user-permissioned access to financial data should and will become a commodity. As a data company, our goal is also to make raw data more readily actionable through enrichment and other tools.

Conclusion

Financial data connectivity is becoming a core component of how financial services are manufactured and delivered. Reports produced by both the Senate of Canada and the advisory committee appointed by the federal Minister of Finance state that a modern data infrastructure is key to the innovation and competitiveness of the financial sector.

There's no question Canada needs a formal open banking system. APIs – should they be well-implemented, and subject to the proper governance – are just a better technology to achieve the same thing as screen scraping. Both connectivity technologies empower consumers with control over their financial data – which in turn gives them access to a broader range of financial products tailored to their needs.

A thoughtful transition requires a nuanced perspective on the current state of financial data connectivity in Canada. Hundreds of financial businesses currently rely on financial connectivity, provided by trusted aggregation providers using screen scraping, to power their daily activities.

> *Ultimately, the value of a formal open banking system is dependent on having the right governance framework in place – one that enables non-traditional participants to bring innovative products to market, one that both protects and empowers consumers as they use their data to access the services they need.*

If Canada succeeds there, screen scraping will become obsolete and go away by itself – take it from a company that has developed and patented a powerful screen scraping technology. 😉