FINANCIAL™
DATA EXCHANGE

Getting Started with Open Banking

A Business Primer by FDX

Executive Summary

Open Banking allows consumers to better manage their financial lives. They have direct access to and can more securely share their data. For financial institutions, open banking enables safe data sharing across the ecosystem to enhance product offerings, streamline new customer onboarding, and improve the overall experience.

Open Banking, also known as Open Finance, enables the secure sharing of financial data through customer permissioned APIs. Financial industry customers benefit by consuming their financial data using their application of choice and by making their data easily portable to new institutions, leading to reduced switching costs.

The financial industry continues to mature on open banking; customers—comprising of consumer, wealth management, and commercial clients—are reaping the benefits. This expanded ecosystem enables automation, security, privacy, and seamless integration across the entire financial services industry.

C-suite executives and boards of directors at financial institutions are asking how their organizations can take advantage of this business model transformation. At the same time, however, these leaders are new to the concept of open banking and do not have a clear understanding of how to initiate an open banking action plan.

Getting Started with Open Banking - *An FDX Business Primer for Financial Institutions* was created to provide a high-level understanding of open banking and help readers begin the process of creating a strategy and business plan to successfully implement open banking. This document addresses general topics related to open banking, provides an understanding of how FDX is positioned within the ecosystem, and is targeted specifically for financial institutions (with a follow-on guide for fintechs planned in the future). While the FDX API may not meet all open banking needs, many of the standards and best practices related to data, consent, and security are applicable across the spectrum of open banking solutions.

The report outlines six key areas for successful open-banking strategic and business planning:

- **Introduction to Open Banking**
- **Examples of Open Banking**
- **North American Open Banking Essentials**
  - **United States**
  - **Canada**
- **Determining Business Value**
- **Establishing an Open Banking Strategy**
- **Developing and Executing a Plan**

Readers will finish with a clear understanding of how to move forward and embrace the future of banking.

FDX is dedicated to unifying the financial sector around a common interoperable standard for the secure and convenient access of permissioned consumer and business financial data.

This document was prepared by the members of the Financial Data Exchange, LLC (FDX), the technical standards body composed of financial institutions, financial technology companies, data access platforms (data aggregators), consumer groups, and industry trade associations participating in the user-permissioned financial data ecosystem. FDX seeks the development and promotion of a common, interoperable, and royalty-free standard—the FDX API (application programming interface)—to facilitate the secure exchange of financial information and accelerate innovation while giving consumers and businesses greater control of their data and better awareness of how their data is being used. This document does not intend to convey or set any policies on behalf of FDX. In the event of any inconsistencies between stated policies and the language of this guide (now or in the future), the FDX stated policies and procedures shall govern in every respect.

Introduction to Open Banking

Open Banking, generally, is an account holder's ability to access their data and financial services through secure and standardized technology channels.

Less formally, open banking enables customers to more securely connect their financial data with an application or lender and have specific control over what is shared and for how long. Additionally, it standardizes data sharing between provider and recipient into a secure technology solution that eliminates screen scraping.

The Challenge

Consumers originally connected their bank data to fintech apps using screen scraping (described below), a practice that originated in the 1990s.

While some fintech apps would connect directly, the typical process was:

1. Users provided their bank login credentials to data access platforms (DAPs).
2. Data access platforms logged in to bank websites using these credentials.
3. Data access platforms extracted user account information from the website ("scraped" off the webpage screen).

The data obtained by the DAP was then available to the user via the fintech app. While generally effective, screen scraping has several challenges:

- **Creates the risk of fraudulent account takeover for both the customer and the bank.**
- **Causes a processing burden on the bank servers being scraped.**
- **Provides no granular access controls specific to data providers.**
- **Maintaining screen scraping integrations is cumbersome and expensive for data access platforms.**

The Solution

Replacing screen scraping with secure, financial grade APIs designed from the ground up for open banking solves these challenges. Secure, permissioned APIs are a better approach as they create a consistent connection, ensure timely data, and help mitigate the risk of inconsistent customer experiences that may result from screen scraping.

In many countries, open banking regulatory and technical standards are being defined by governmental regulation and have the primary elements of financial data portability and account holder payment initiation. The regulatory environment in North America is still evolving with key rules being drafted at the time of this document. However, the private sectors in U.S. and Canada have made significant strides creating technical standards for open banking through the Financial Data Exchange consortium. FDX is dedicated to unifying the financial sector around a common, interoperable technical standard for the secure and convenient access of permissioned consumer and business financial data using the FDX API.

Beyond Consumer Banking

The open banking ecosystem is evolving beyond retail bank data sharing to include open finance, embedded finance, Banking-as-a-Service (BaaS), and other emerging practices. Each of these approaches requires an evaluation of technical needs, business models, and compliance considerations beyond FDX standards.

The term "open banking" entered the industry lexicon in 2016 with the UK's Competition and Markets Authority "Retail Banking Market Investigation." The concept of open banking was originally intended to increase competition by enabling consumers and small businesses to share data and initiate payments with trusted third parties. The CMA and the nine largest banks in the UK established the Open Banking Implementation Entity (OBIE) to create UK standards for open banking.

Open Finance is an extension of open banking, moving beyond consumer banking accounts into loans, investments, small business, and other accounts. Open finance currently includes data sharing to enable products like lending, foreign exchange services, commercial cards, and cryptocurrency.

Open finance is expected to eventually include most financial services and products. The CMA released "The Future Oversight of the CMA's Open Banking Remedies," which outlines plans to replace the OBIE with a future entity tasked with expanding UK standards to includes open finance.

In North America, the term "open banking" is not limited by regulations that limit the scope of customer data and payments. Open banking and open finance are often used interchangeably.

Embedded Finance roots bank services into a customer experience, such as a mobile application, website, or third-party software. Consider, for example, a rideshare application that allows for payments once the ride is complete. The payments service is embedded in the rideshare app by integrating with a financial institution's APIs.

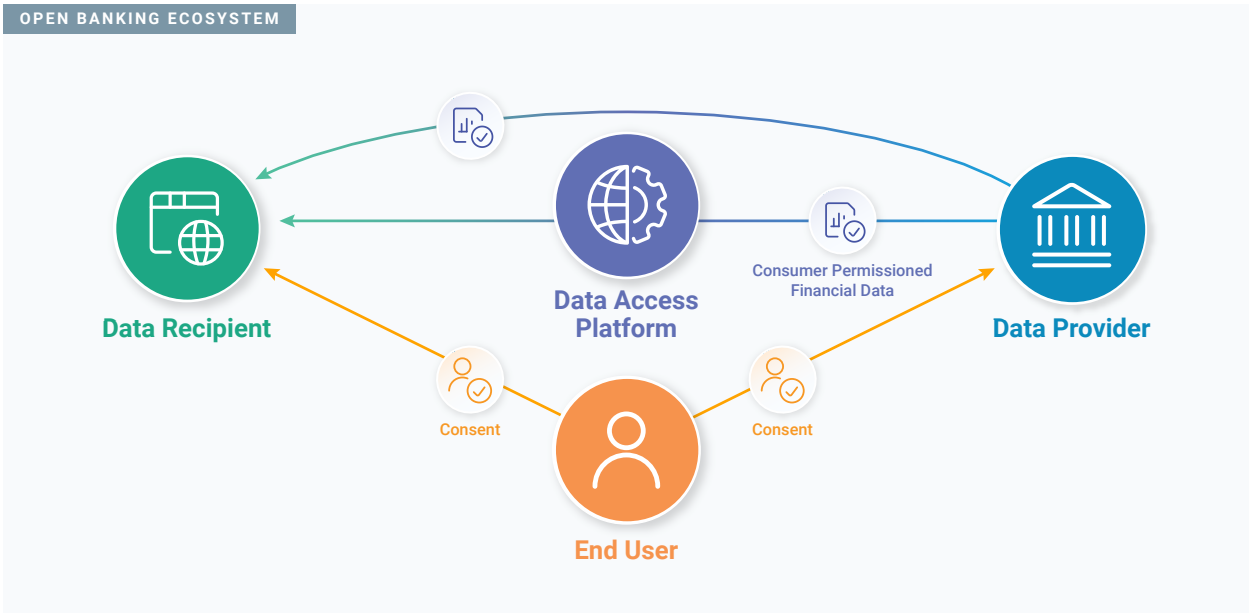
Buy-Now-Pay-Later (BNPL) is another example of how APIs enable businesses to embed the service at the point of sale. Commercial bank customers and third-party bank partners, such as fintechs, are increasingly using embedded finance.

Banking-as-a-Service (BaaS) offers licensed bank products and services on digital marketplaces, through independent software vendors, or third-party partners, enabled by open banking infrastructure. While BaaS is part of the open banking ecosystem, there are compliance, technical, and strategic partnership considerations that go beyond basic open banking.

BaaS is a wholesale distribution model for open banking products and services. In this distribution model, API products are often competing in a marketplace among multiple banks. This model does not require a direct relationship between the ultimate client and the bank.

Examples of Open Banking

Open banking benefits consumers, small businesses, large corporations, capital markets, and wealth management. There are many open banking use cases, but a few simple examples aptly illustrate the shared value of open banking for both account holders and financial institutions.



Consumers and Individuals

Retail bank customers benefit when they can use their choice of fintech application to check account balances or transfer money. Open banking enables a wide variety of applications for consumers to broaden access and fuels innovation. Without open banking APIs, account holder frustration increases when third-party applications cannot reliably connect to their bank, the data is not timely, or an established connection breaks. Often, these customer frustrations are directed at the bank for not having the appropriate capabilities in place to empower the technologically-driven economy.

Open banking APIs allow individuals to share their financial data with a fintech application without having to share usernames or passwords with a third party. They eliminate screen scraping, which creates a processing burden on bank servers and is prone to malfunctioning when websites are updated. APIs are more reliable, are customer-permissioned, enable real-time data sharing, and provide financial institutions more robust capabilities for capturing customer consent to share data. Moreover, financial grade APIs are designed from the ground up to support open banking, giving financial institutions confidence in the security and privacy of the solution.

Commercial and Business Clients

Commercial customers benefit from open banking by automatically pulling their daily balances into Enterprise Resource Planning (ERP) systems via open banking APIs. Standardized, interoperable, open banking APIs create streamlined, lower-cost implementations for all parties involved. The ERPs use open banking APIs to, among other things, manage cash positions in real time, automate reconciliation across subsidiaries, manage payments to suppliers, and match invoices to payments.

Commercial clients can also deliver value to their customers using open banking by embedding bank services into their website and mobile applications. Embedded finance allows commercial clients to offer digital experiences and frictionless commerce.

Wealth Management Clients

Private wealth management clients benefit from open banking by being able to connect their accounts across all institutions securely to understand the entirety of their financial positions in real time.

Historically, wealth managers gained a holistic view of a client's financial positions through a combination of advisor logon and paper statements, which were inefficient, less accurate, and untimely.

North American Open Banking Essentials

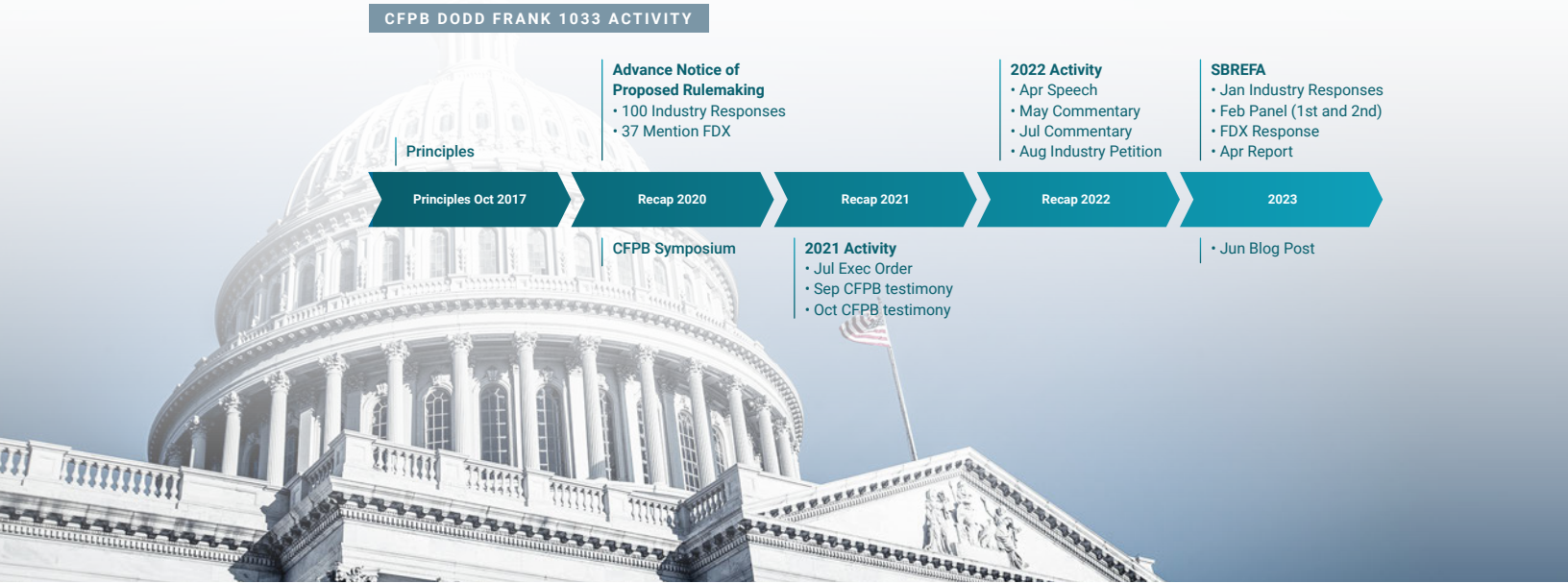
To be successful at open banking, business leaders should form an understanding of the history of open banking in North America, including the different approaches by the United States and Canada, for compliance, legal, privacy, and security risk management.

A Brief History of Open Banking in the United States

The groundwork for regulated open banking in the United States was laid with the passage of the Dodd–Frank Wall Street Reform and Consumer Protection Act in 2010. This Act instructed financial institutions to make consumers' financial information available to them in digital formats. As of this report's publication date, the related CFPB rule making is still in process. To date, the majority of U.S. open banking standards have been driven by the private sector. The U.S. open banking standards will continue to evolve due to emerging regulatory and industry expectations around data portability, security, and privacy.

The U.S. progression differs significantly from open banking in the United Kingdom, the European Union, and Australia, where open banking technical standards have been defined by regulators. The early focus of open banking in the United States has been to protect consumer banking customers. The first objectives were to make data sharing with data access platforms and fintech companies secure, permissioned, interoperable and in alignment with data privacy principles.

In 2017, the Consumer Financial Protection Bureau (CFPB) released Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation. The CFPB principles are not regulatory guidance but emphasize the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-permissioned use of financial data. There are nine (9) principles in total. APIs are not specifically mentioned; however, APIs would meet the expectations laid out in the CFPB principles.



FDX had its origins in 2017 as well. It started as a grassroots effort led by financial institutions, fintechs, and data access platforms seeking common ground for a secure, consumer-centric data sharing framework. Recognizing the considerable progress made from 2015–2017 by the FS-ISAC Aggregation Working Group with its Durable Data Application Programming Interface (DDA) standard, FDX became a wholly-owned, independent subsidiary of FS-ISAC in 2018. FS-ISAC assigned all versions of the DDA (now known as the FDX API) to FDX in October 2018 in connection with FDX's launch.

"This customer-permissioned access to data through the APIs is the key benefit and business value for providing open banking to consumer clients . . . "

- Don Cardinal, Managing Director
Financial Data Exchange

U.S. Compliance and Legal Risk

Individual consumer bank clients use open banking to obtain secure data portability and payments. This customer-permissioned access to data through the APIs a key benefit and business value for providing open banking to consumer clients and is

FDX is a nonprofit organization operating in the United States and Canada dedicated to unifying the financial services ecosystem around a common, interoperable, and royalty-free technical standard for the secure and convenient access of permissioned consumer and business financial data, aptly named the FDX Application Programming Interface (FDX API).

FDX is governed by a diverse board of directors from across the financial services ecosystem, and it has a global membership that includes financial institutions, financial data access platforms, fintechs, industry utilities, payment networks, consumer groups, financial industry groups, and other stakeholders involved in user-permissioned financial data sharing.

The FDX API is adopted, in part, to migrate away from screen scraping and has become the most widely used open banking API in the United States and Canada. The FDX API has been widely adopted across the industry and positively impacts tens of millions of customer accounts.

The FDX API is free to access and use subject to the terms of the FDX API License Agreement. FDX members have access to additional participation rights and documentation containing best practices around risk, controls, user experience, and other open banking topics.

While the FDX API is a key component to any open banking strategy, it is not a panacea for all data sharing needs. Commercial customers, institutional wealth management clients, and other customers have shown a demand for premium APIs that support ERP automation, embedded finance, and other commercial demands. These premium APIs can leverage multiple components of the FDX API, and the consortium is exploring other ways to foster innovation in the commercial space.

closely tied to risk management and compliance. The UK and other countries have already regulated open banking through a technical standard; in the United States, industry-led standards through FDX have preceded regulation and will ideally benefit compliance with regulations as they are adopted.

There is a White House focus on open markets and competition, as expressed in an executive order issued by President Biden. The Executive Order on Promoting Competition in the American Economy references open banking, data portability, and Dodd-Frank §1033.

The Order states that rulemaking should facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products.

The CFPB is actively undergoing rulemaking for Dodd-Frank §1033, which they indicate will be published in Q4 2023.

Additionally, proposed third-party risk management guidance from the Federal Reserve, OCC and FDIC begins to outline requirements and address early industry questions around open banking, specifically around the consumption of alternative data from DAPs and open finance APIs. A key point to highlight is that, under current OCC and FDIC guidelines, data access platforms are likely to be considered part of a third-party business arrangement if there is any contractual agreement or bilateral data-sharing agreement in place.

This is true even if:

- **There is no financial benefit to the financial institution.**
- **The customer permissions the data sharing with data access platforms**.

Typically, the transition from screen scraping to open banking overlaps and both APIs and screen scraping are used simultaneously. Practitioners should work with their legal and compliance departments to understand the regulatory requirements for data sharing using APIs and screen scraping.

". . . there was universal agreement . . . APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping"
U.S. Treasury, 2018

U.S. Risk Management: Privacy and Security

A key privacy and security challenge of open banking in the United States is the historical and still-persistent use of screen scraping to collect consumer financial data. Historically, without APIs or data sharing agreements between financial institutions and data access platforms, account holders would be prompted to provide their login credentials. The sharing of login credentials with third parties increases the risk of fraud and privacy breaches.

Data access platforms and banks are working to give consumers and financial institutions enhanced control over data

sharing (whether through APIs, bilateral data sharing agreements, or screen scraping). Privacy, customer permission, and security are all engineered into the FDX API solution, thereby reducing the potential for fraud and cybersecurity attacks.

FDX promotes technical standards to ensure that financial APIs are both secure and permissioned by incorporating modern security technologies and protocols. The FDX standards include employing OAuth 2.0, OpenID Connect (OIDC), and mutual transport layer security (mTLS) (together, the FAPI authentication protocol). Additionally, the FDX consortium organizes industry working groups to create best practices around financial APIs to further promote innovation and to continue to protect the customer.

"An effective way to improve the privacy and security for the customer is through bank investment in new authentication security tools and financial grade APIs."
U.S. Treasury, 2018

A Brief History of Open Banking in Canada

As in the United States, Canadian open banking efforts have largely been driven by the private sector. Unlike the United States, however, various government bodies have been involved with open banking for several years, culminating in 2021 with a formal recommendation from the Department of Finance Canada. The recommendation included broad goals, a proposed timeline, and the appointment of an open banking lead. This government involvement makes the Canadian approach more of a blend between market-driven and regulatory-led solutions. While both countries share a common goal of keeping consumer bank data safe by eliminating screen scraping and instituting security protocols, the Canadian approach emphasizes the overall systemic risk as well.

In 2018, open banking activity began in earnest by both the private and public sectors. A group of senior subject matter experts from Canada's leading financial institutions created a working group to address challenges and opportunities posed by open banking and propose an industry-led data sharing reference model intended to create a solution for the marketplace. The goal was to ensure an efficient, safe, competitive, and innovative ecosystem that provides value and choice for Canadian consumers. Separately, the government formed the Advisory Committee on Open Banking to explore a regulatory approach, resulting in the publication of a January 2019 report: "A Review into the Merits of Open Banking." The report was opened for public comment and generated a great deal of feedback from diverse points of view.

In late 2019, FDX began discussions with key Canadian stakeholders in Canada to form a working group within FDX that would unify Canadian financial and fintech leaders. The FDX Canada Working Group Charter was finalized in March 2020. Sustaining members were elected later that year, which led to the beginning of a common, standards-driven approach within the private sector. In July 2020, FDX officially launched in Canada. In January 2020, the Canadian government's Advisory

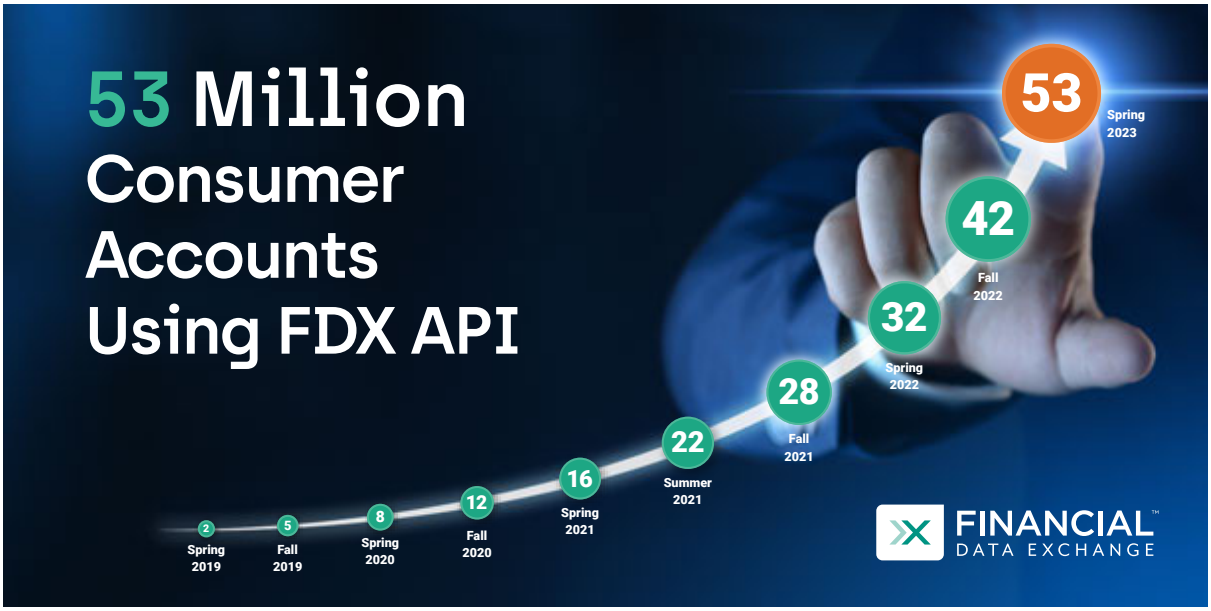
Committee published "Consumer-Directed Finance: The Future of Financial Services", a follow-on report to "A Review into the Merits of Open Banking" that strongly recommended moving forward with open banking, leading to another round of industry consultations.

In August 2021, the Advisory Committee released its Final Report, clearly outlining their recommendations on how to move forward with open banking by allowing consumers and small businesses to permission sharing their data in a safe and efficient manner to access useful products and services without the use of screen scraping.

The report includes a timeline that divides the roadmap into two phases, (1) Establish (subdivided into Design and Implementation) and (2) Review, with a target live date of January 2023.

Since the publication of the Final Report, FDX Canada has continued to grow its membership. There are currently over 60 Canadian financial industry organizations who are members of the working group, including every major incumbent bank, credit unions, several challenger banks, and many prominent fintechs.

Beyond enlisting a broad and prominent pool of members, FDX Canada has begun to extend the FDX standard to meet Canadian requirements. In October 2021, the release of v5.0 of the FDX API marked the first inclusion of Canadian specific data elements. Future releases will extend the standard further to include Canada-specific investment and account type data elements, and other elements identified by Canadian members. Such ongoing updates recommended by the FDX Canada working group demonstrate a commitment to ensuring that uniquely Canadian market



requirements are accurately reflected in the development and maintenance of the FDX API standard. Moreover, these changes are directly driven by working group participants. Additionally, in January 2023, FDX amended the FDX Canada working group charter to provide that working group with certain self-governing implementations of API government required extensions without the need for approval from FDX global.

While the United States and Canada view the elimination of screen scraping as a key goal, Canada has an increased emphasis on providing consumer control over data sharing, as evidenced by the adoption of the term consumer-directed finance.

To that end, consumer control and permissioning of data can be strengthened by adoption of the FDX API. Through broad adoption of the FDX API, it is a possible for the flow of user-permissioned data between financial institutions, financial data access platforms, fintechs, payment networks, consumer groups, financial industry groups and other permissioned parties in the financial data ecosystem to be more secure, reliable, and fundamentally consumer-directed.

As in America, Canada has been exploring open banking scenarios beyond those addressed by the FDX API. Both private sector and government stakeholders have continually highlighted the opportunities open banking can bring to the small-and-mid-sized (SME) business sector. Independent of regulatory movement, Canadian financial players are looking beyond compliance to the commercial opportunities made available by open banking, like their peers in the U.S. market. FDX Canada, like its U.S. equivalent, is exploring how to extend the FDX API to foster innovation in these new areas to better serve the financial consumers.

Canadian Compliance and Legal Risk

The 2021 Final Report from the Advisory Committee on Open Banking represents the blueprint guiding Finance Canada's efforts to implement open banking. The exhaustive and precise report contains 34 recommendations regarding the various features of Canada's envisioned open banking regime.

The recommendations are organized into six categories:

- **Vision**
- **Scope**
- **Governance**
- **Common Rules**
- **Accreditation**
- **Technical Specifications and Standards**

The report explicitly recommends a blend between government- and industry-led approaches, with the aim of establishing a hybrid, made-in-Canada approach focused on three foundational elements: **Common Rules, Accreditation, and Technical Specifications.**

Included in the report is an 18-month timeline for Phase One: Design and Implementation. The first nine months are allotted for Design, with the aim of authoring a framework to guide the early implementation of the system.

The second nine months apply to Implementation, whereby the system is built and tested by service providers (to include seeking formal accreditation). The 18-month timeframe began with the naming of Abraham Tachjian as Canada's open banking lead in March 2022. Therefore, although the report initially called for a live date of January 2023, the actual target live date for an initial implementation is currently projected to be September 2023.

The report highlights the elimination of screen scraping as a clear goal for the initial phase. However, it also includes broader, longer-term outcomes that are focused on consumer data protection and control, the need to enable innovation and competition, and mechanisms to facilitate liability and recourse.

For FDX purposes, the report recommends a market-led effort to develop a technical specification during the first nine months of Design, with the goal of aligning to the following principles:

- **Accessible and inclusive**
- **Positive consumer experience**
- **Safe and efficient**
- **Capable of evolving**
- **Sufficiently flexible**
- **Compatible and interoperable**

The FDX API already largely aligns with these principles, and FDX Canada continues to develop the standard with these principles firmly in mind.

Canadian Risk Management: Privacy and Security

In Canada, the desire to transition beyond screen scraping has been prominent from early open banking efforts all the way through to the Advisory Committee's Final Report. The Canadian financial sector is well known for being risk-averse, so the fact that screen scraping leads to the sharing of banking credentials with unregulated entities raised immediate concerns. However, consumers demonstrated overwhelming demand for the services that screen scraping enabled, with over four million Canadians willingly sharing their credentials, despite the risk of security breaches. Meeting this demand in a secure and reliable manner quickly became one of the main drivers of open banking in Canada

Further, privacy for open banking is being developed in concert with other digital privacy initiatives, such as Bill 64 in the province of Quebec. In 2019, the Canadian government introduced Bill C-11, a significant modernization of the longstanding Personal Information Protection and Electronic Documents Act (PIPEDA), including provisions on data sharing, privacy, and consent. Unfortunately, Bill C-11 did not pass, but in June 2022, the government introduced Bill C-27 which significantly improved upon the original by introducing requirements for privacy policies, levels of protection, notification capabilities, transparency, and consent management. It is generally understood that the provisions in C-27 are intended to support the open banking initiative running in parallel. If the legislation passes, it will impose significant new privacy requirements on the banks. However, the extensions they must make to their privacy and security facilities will act as a strong

foundation for the introduction of open banking capabilities.

While open banking API standards may differ from region to region, the underlying security mechanisms are largely the same. The modern security protocols supported by the FDX API, including OAuth 2.0, OIDC, mTLS, FAPI 1.0 Advanced and CIBA, represent a common set of technologies used by virtually all open banking regimes around the world. As a result, there is likely to be little deviation between FDX implementations in Canada, the U.S. and other jurisdictions when it comes to the security mechanisms. Even in highly regulated open banking regions, these same technologies are used to protect the privacy of consumers while still enabling them to securely share their financial data based on explicit consent, without the need to share banking credentials.

Determining Business Value

The open banking ecosystem in the United States has been driven by private sector innovation and is delivering real value to bank customers. Open banking enables financial institutions to generate business value through novel customer experiences, real-time capabilities, embedded finance, and other innovation that generate value.

Customer Experience

Open banking is improving the customer experience through fintech apps, bank websites, and bank mobile applications. Open banking was initially one directional data sharing where data access platforms primarily captured financial data for fintech applications. The improved customer experiences created by fintech companies are widely known.

The industry has now moved towards bi-directional data sharing through which a bank can push or pull data. Financial institutions can accomplish this through APIs by partnering with data access platforms or open banking networks.

The demand to pull data into banks has led DAPs to offer data augmentation services that enrich data across the entire financial ecosystem. This enriched data provides both the bank and the customer with valuable information that improves the customer experience.

Open banking APIs offer multiple improvements over screen scraping for financial institutions, data access platforms, and fintech applications. Open banking also provides more protection and control to the underlying bank customers. The value chain begins and ends with the underlying customers demanding financial services. Fintech companies create value in many ways, including providing novel experiences, financial insights, and convenience. Data access platforms help both financial institutions and fintech companies create reach through large networks across institutions. Data access platforms also provide value-added services that benefit the developer community, banks, and the underlying customers.

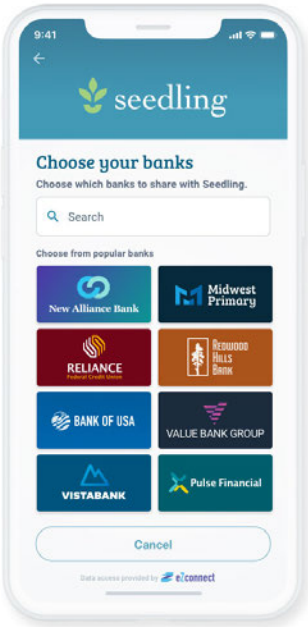
Open banking APIs are more reliable, secure, and transparent than screen scraping which benefits all stakeholders and customers. Open banking increases availability and quality of data throughout the ecosystem. Additionally, all stakeholders are better positioned to meet evolving regulatory and customer expectations through open banking APIs.

Example:

Consider the modern complexities of a bank customer who utilizes multiple financial institutions and is applying for credit at their primary bank. The customer may pay their bills (credit cards, rent, and utilities) through their primary checking account but may also have accounts at other financial institutions with investments, loans, or other income generated from different sources.

In this example, gig economy income may not be recognized through traditional income verification methods, and some assets may not be readily available to banks during the underwriting process. This creates a situation in which banks may not be able to make a credit offering competitive with that offered by fintech companies due to limited insight into the customer's holistic financial picture.

However, DAPs have developed connections to most financial institutions and have solutions that analyze bank transactions to recognize sources of alternative income and assets held at other financial industry participants. These data enhancements, combined with open banking APIs, provide a more complete picture of the customer's financial situation, and allow banks to offer more competitive offerings as part of an automated underwriting process.



Real-time Capabilities

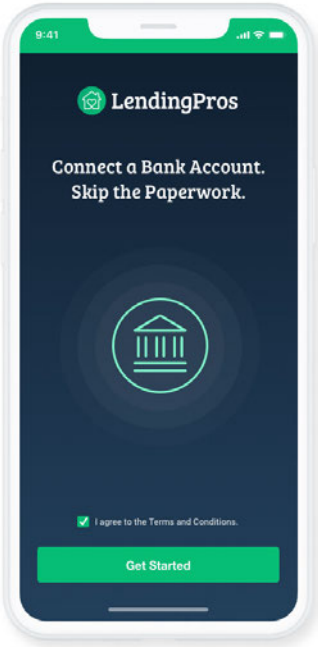
The use of APIs for data sharing allows for on-demand data transfer and real-time customer experiences. Creating real-time processes and customer experiences will require an evaluation of the supporting technology and data processes to ensure speed and dependability. Real-time processes across multiple institutions within an open banking network will require coordinated support across institutions.

Example

A customer wants to apply for a mortgage loan with their bank. The bank would traditionally ask for a multitude of statements and verifications that are manually provided by the customer. The bank would then manually collect data from these documents and key them into the mortgage application system. These processes could take days or even weeks. Re-key errors and errors from optical character recognition (OCR) further complicate the process. Real-time APIs eliminate these errors and delays.

Via APIs, these statements are available directly from the financial institution and do not pass through the borrower—eliminating chain of custody issues as well.

Open banking reduces the burden on the customer and allows the bank to automatically complete these processes in real-time by partnering with data access platforms or open banking networks. In this example, open banking leads to an improved customer experience, faster loan decisions and eliminates manual steps for both the bank customer and the financial institution.



Embedded Finance

Open banking allows commercial clients and third-party partners to embed bank services into websites and applications. Embedded finance solutions allow bank services to be used on-demand as part of a larger digital solution. These automated processes can be back-office or part of a user experience.

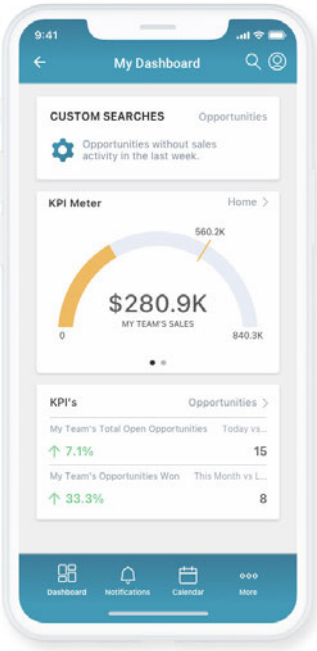
Example

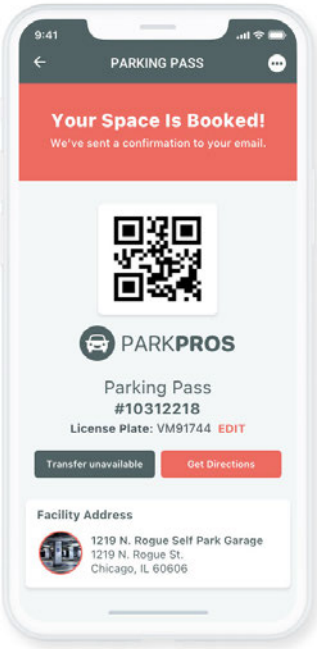
Commercial bank clients use ERP applications to manage their supply chain and customer relationships. Commercial clients want to automate their back-office processes using their ERPs and open banking APIs. Traditionally, ERP users must manually download bank files and perform manual reconciliations with invoices. These steps can be fully automated using open banking APIs, allowing commercial clients to focus their time on higher value activities.

Commercial clients and third-party partners create novel digital experiences for their customers by embedding bank services into their websites and mobile applications. Many mobile applications have payment capabilities powered by open banking APIs. These applications have enabled the gig economy and applications powered by AI that create convenience.

Example

A smart parking app recognizes that a car is in a pay space, prompts the user to estimate how long they will need the space, and recommends that the driver authorize a real-time payment to the appropriate parking authority. In this example, a bank's payment rails are embedded within the smart parking application and become central to the commercial client's business model.





Monetization of Open Finance APIs

Some financial institutions have aggressively pursued an open banking business model to generate revenue from commercial clients who want to innovate on top of open banking APIs.

Open banking generates revenue from business customers in four primary ways:

- **New client acquisition**
- **Deepening existing client relationships**
- **New digital products**
- **Usage fees**

Banks are attracting new customers and generating revenue by offering open banking products to business clients. These products can be simple bank services, such as payment initiation through APIs, or complex products that incorporate AI. Some examples of AI-enabled open banking products include "smart" payment rails that automatically determine optimal payment options or a real time fraud prevention solution. Regardless of complexity, API financial products are designed to be part of an integrated digital customer experience.

Lastly, banks can charge their business clients for using premium open banking APIs. These fees are typically based on usage volume and the risk of the service offered. For example, Real-time payments would cost more than a data service that provides current balance due to differences in risk.

Establishing an Open Banking Strategy

An open banking strategy must align to an organization's enterprise strategy, position the organization relative to competitors, and have measurable goals.

The strategy should consider the rapid pace of FDX adoption among all stakeholders across the U.S. financial ecosystem. Additionally, the strategy should understand the unique needs across customer types (commercial, retail, wealth management, and so on). In general, bank customers increasingly expect real-time services that are secure and permissioned, thus requiring open banking APIs.

Goal Setting

Open banking will impact most areas of an organization and will require well-thought-out goals at both the enterprise and team levels. Clear goals help an organization create alignment and shared expectations. Each FI will have unique business objectives that will impact their strategic goals. Examples of well-defined open banking goals include:

1. Setting an institutional philosophy on customer data sharing that can be reflected within legal data sharing agreements.
2. Assessing industry trends and performing a competitive analysis among banks, fintechs, and large technology firms.
3. Selecting open banking business models. In addition to compliance expectations, will the organization focus solely on eliminating screen scraping or will it offer premium APIs as well.
4. Educating internal stakeholders and creating awareness.
5. Determining the organization's risk appetite and risk capacity related to open banking and screen scraping.
6. Assessing how Open Banking and APIs fit together, whether as a channel, a product strategy, or part of the enterprise roadmap.
7. Performing an open banking gap analysis and related action plan.
8. Identifying targeted customers and related business models.
9. Performing customer surveys.
10. Creating a technical and business roadmap that scales with customer demand.

Identifying Internal and External Stakeholders and Their Priorities

At a high level, open banking could impact all parts of an organization. To make progress, a core group should be identified that aligns business, compliance, and technological interests. External stakeholders can be identified by joining industry groups and identifying data access platforms who currently connect to financial institution's website and mobile platforms.

The following is a list of potential activities that can be used to engage stakeholders across the organization in promoting the success of an open banking implementation plan:

1. Data Sharing Agreement
Establish a cross-functional team to form and negotiate data sharing agreements. Standards bodies like FDX often have member-contributed material that can help inform and potentially accelerate the contract process. Trade associations and other industry groups may have templates for data sharing as well.

2. Standards
Determine the technical standards (like FDX) that will impact the open banking program and initiatives.

3. Customer Support
Empower customer-facing teams to communicate value, answer questions, and meet customer expectations. Create processes for resolving customer disputes or complaints for processes that involve multiple organizations in an open banking network.

4. Business Intelligence
Determine how the organization will collect, analyze, and drive business value using open banking data.

5. Enterprise IT
Determine the impacts, needed technology enablers, and resource capacity requirements. Examples of key external technology stakeholders are Core Processors and CIAM (Customer Identity and Access Management) providers.

6. Procurement
Partner with procurement to determine if the current procurement process will support an open banking business model.

7. Migration Impact
Identify existing internal processes that rely on screen scraping or data access platforms services as well as legacy/proprietary APIs.

8. OFX Impact
The Open Financial Exchange (OFX) API is actively deployed at over 7,000 institutions and may accelerate a company's journey to the FDX API. The OFX Consortium joined the FDX Data Exchange (FDX) in 2019 and formed the OFX Working Group to ensure that the use cases supported by OFX are also supported by the FDX API. The working group is also creating material for members to accelerate voluntary migration from OFX to the FDX standard. Execution teams should identify and engage internal and external stakeholders who currently use legacy OFX APIs.

9. Mutual Roadmaps
Engage data access platforms to establish mutual plans for migrating from screen scraping to an open banking API.

Identifying External Standards

As highlighted in this report, FDX is the primary North American body creating standards for interoperable open finance APIs. There are multiple domestic and international organizations that create standards that impact open banking, such as the National Institute of Standards and Technology (NIST), Open Finance Data Security Standard (OFDSS), and the OpenID Foundation (OIDF). Financial institutions should form cross-functional teams that research industry standards and determine gaps relevant to open banking.

Developing Strategic Partnerships

A successful open banking strategy will require internal and external strategic partnerships. A best practice is to establish an internal executive sponsor and leadership group that will oversee and drive open banking for the organization. This internal team must be cross-functional and should include members from technology, digital, legal, compliance, risk management, data, and business teams.

Open banking will also require strategic partnerships that align with strategic goals, targeted customers, and gap assessments. Organizations will have to determine build versus buy decisions in a way that creates scale and sustainability. External strategic partnerships will be key to delivering value to open banking customers.

Developing and Executing a Plan

Organizations should create an open banking plan designed to accomplish their strategic goals.

This section provides a high-level approach for migrating away from screen scraping and for creating premium APIs.

Both the FDX and premium commercial APIs will require common technological enablers such as modern authentication, an externally facing developer portal, and cloud infrastructure. Utilize the gap analysis to determine the specific enabling technologies needed. Business leaders should complete a build-versus-buy analysis that evaluates the timing of needs, maintainability, internal expertise, vendor expertise, and the extensibility and interoperability of vendor solutions.

Migrating Away from Screen Scraping

First, **create a plan** for data-out and data-in and ensure that these two plans align to support a cohesive open banking data strategy. **Identify strategic partners** for both data-in and data-out and create a mutual project plan.

The **FDX API** should be a principal component of the data-out strategy. Because the FDX API is a standard, the project team should **evaluate whether to build or buy the API**. Additionally, the project team may consider an open banking developer portal that comes with pre-existing FDX API endpoints. Developer portals can be built in-house or Software-as-a-Service (SaaS). The SaaS approach could alleviate the burden of versioning the FDX API from banks. Note, a SaaS approach does not remove the requirements of the bank to maintain and version their data model that feeds the API.

Project teams should begin **creating business requirements around the FDX APIs**. The business should determine if they will implement the entire FDX data model or only part of the data model, and whether custom fields will be required. A **migration plan** should ensure that all fields currently available for screen scraping are also available in the first version of the FDX API. Additionally, review any excluded fields with data access platforms to understand the impact on fintech apps and bank customers.

The project teams must understand how the bank will **manage consent flow** for their clients. Consent management is how a user authorizes permission and manages third parties allowed to use their financial data. Consent can be managed by the user at the DAP, by the user via a bank application, or by the bank itself in aggregate with a third-party or fourth-party connection. The project team must consider their **consent management path** to appropriately design data sharing agreements and to facilitate risk management of customer data.

Next, **begin negotiating data sharing agreements** with data access platform or other recipients. API business models may cause organizations to consider having data sharing agreements and an onboarding process for all users of the API. There are some open banking networks that use

multilateral agreements, but not all of the major data access platforms are on these networks. Most banks will find that they will need a combination of multilateral and bilateral data sharing agreements.

Once the data sharing agreements are in place, the bank should **choose an initial testing** partner to ensure that the FDX API is working appropriately, and that the data is timely. This can be a DAP partner or a pool of clients that support innovation or are willing to evaluate with the bank.

The bank should also **create a process for communicating** and responding to problems. The customers' most common call will be to their financial institution if something breaks. Financial institutions should establish processes to coordinate with data access platforms and other stakeholders to resolve customer issues as they arise.

The FDX API should be used in production for a predetermined amount of time prior to shutting off screen scraping to ensure proper functioning and scaling. Parallel processing is a common redundancy control in major conversions and is considered a best practice. Banks should **create multiple feedback loops** to ensure proper coverage and reduce the risk of customers losing connectivity to their favorite fintech or payment app.

FDX Certification

At the time of this writing, the FDX certification is in the Beta phase and expected to be rolled out in early 2024. Bank leaders should understand and socialize the value of the FDX API Certification. Banks who become certified communicate clearly to the market that they are quality innovation partners who hold themselves to a high standard for protecting customer data and privacy. The FDX Certification may signal to regulators that the bank effectively supports customer data portability while meeting a minimum set of standards for data management, customer privacy, risk management controls, and authorization capabilities.

Premium Commercial APIs

There is an increasing need to meet business client demands through enhanced data and API offerings. Premium commercial APIs are a type of digital banking product focused on the value of data for bank clients.

Banks should **partner with clients** to form an innovation partnership to deliver premium commercial APIs. While some commercial banking APIs have been around for years, adoption has been varied based on customer demand and product complexity. To increase adoption, banks should collaborate with clients to **develop these APIs** so that they can receive timely feedback and iterate with the client. These clients can be thought of as innovation partners and are key to successful execution of a premium API strategy. Banks should look for tech-savvy clients who are already using financial APIs or clients who are willing to evaluate APIs within their ERPs or other applications.

Once a set of innovation partners has been identified, the bank can **negotiate a customer agreement** that protects the customer and the bank and begin aligning

on timeline and project expectations. Banks should utilize the **FDX standards** where appropriate when building these premium APIs. FDX has standards that may impact data definitions, formatting, security, and consent.

Example

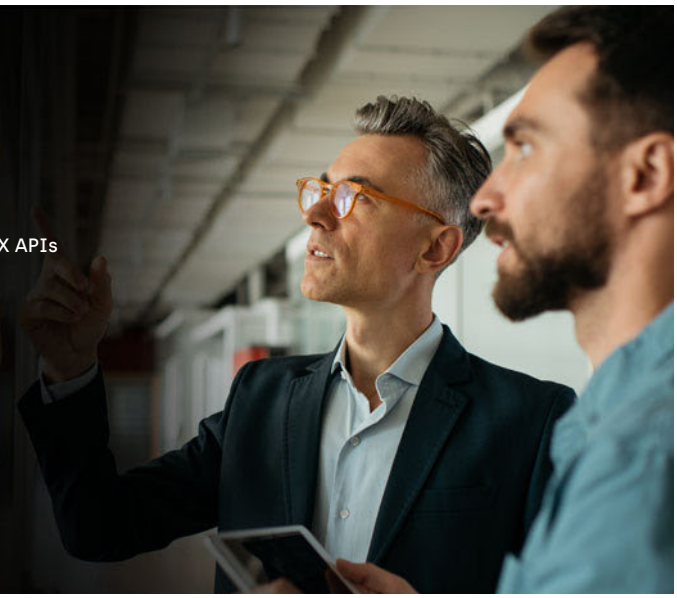
Consider a business client with multiple bank accounts and multiple ERP systems. Without any APIs, the client is using batch file transfers and manual processes to ensure that their ERPs stay synchronized with their bank activity. This traditional approach is resource-intensive, increases the chance for errors, and requires regular maintenance. Multiple ERPs and subsidiaries found at most large corporate clients compounds the complexity and increases the need for open banking.

Large corporations can automate a range of complex processes across subsidiaries by using bank APIs, ERP APIs, and middleware that scales bank integrations across multiple ERPs. The end goal is to improve and simplify customer processes with embedded finance enabled by open banking infrastructure. Banks can create scale by collaborating with innovative third-party partners to simplify customer onboarding and reduce the burden on bank IT teams.

As the open banking ecosystem matures, additional commercial API offerings that build upon the current ecosystem and FDX APIs will emerge. These commercial and emerging APIs may be some of the biggest monetization opportunities and imperative customer acquisition and retention. With any new product, client iteration with an innovation partner is critical to ensure products are viable and scalable.

Developing a Plan of Execution

1. Create a plan
2. Evaluate whether to build or buy the API
3. Create business requirements around the FDX APIs
4. Manage consent flow
5. Negotiate data sharing agreements
6. Choose initial testing partner
7. Create process for communicating
8. Create multiple feedback loops
9. Partner with right clients
10. Collaborate with clients to develop APIs
11. Negotiate customer agreements



Conclusion

The transition from zero to open banking hero is one that most banks face in the natural progression of digital transformation of bank channels and products, but there is no need to feel overwhelmed or alone in the process.

Successful open banking programs will discern the context of open banking, understand customer needs, identify value drivers, navigate dynamic legal and compliance requirements, and successfully execute on a business centric strategy.

While open banking is new and not necessarily straightforward to the casual observer, creating business value from the portability of data and supporting embedded finance is the next phase for servicing bank customers. The information provided in this report has provided the foundational basis for successful open-banking strategic and business planning and is a valuable resource for executives looking to move their businesses into the future of the financial industry.

Facts on Open Banking

Key Industry Stakeholders
Open banking in North America is industry-led and consists of financial institutions, fintechs, data access platforms (data aggregators), and industry groups. See the FDX Registry and the Financial Data Exchange (FDX) website.

Open Banking versus Open Finance
The key domains of open banking may be defined by regulation in some countries and typically include financial data portability and payments. Open banking often refers to consumer deposit accounts; open finance encompasses all other financial use cases.

The Impact of Open Banking
Open finance impacts most bank clients, with the largest share representing consumers (retail, small-business, and private wealth management). This customer group is the most reliant on fintech mobile apps and tools to consolidate financial accounts, and/or facilitate transfers and payments.

When replacing screen-scraping with secured APIs, the transition must be implemented while ensuring ongoing functionality for these customers. Other clients, such as commercial banking clients will also be impacted as they continue to integrate their enterprise resource planning (ERP) systems, websites, and customer-facing mobile apps with banks using APIs.

Open Banking Increases Security
The transition from screen scraping to modern, financial-grade APIs allows for the secure and permissioned exchange of information, which is vital to the financial ecosystem. It better protects consumers and other stakeholders compared to uncontrolled screen scraping from bank websites with users' login credentials.

Active Regulatory Space
In November 2020, the Consumer Financial Protection Bureau (CFPB) released an Advanced Notice of Proposed Rulemaking (ANPR) related to Dodd-Frank §1033 that is expected to eliminate screen scraping and create standard requirements around consumer data sharing. The release of the Proposed Rule is expected in Q4 2023. The ANPR is further supported by President Biden's July 9, 2021 executive order stating that the CFPB should continue rulemaking under Dodd-Frank §1033 to facilitate the portability of consumer financial transaction data.

On July 13, 2021, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporate (FDIC), and Office of the Comptroller of the Currency (OCC) requested comment on the proposed changes to third-party risk management guidance. The proposed changes included a statement that banks should take steps to manage the safety and soundness of the sharing of customer-permissioned data with third parties.

On August 12, 2021, the Federal Financial Institutions Examination Council (FFIEC) released cybersecurity guidance stating banks should maintain a comprehensive risk management program that includes an assessment of risks and effective mitigating controls for credential and API-based authentication.

On September 21, 2021, The U.S. House Committee on Financial Services held a hearing titled Preserving the Right of Consumers to Access Personal Financial Data. Multiple speakers, including a representative of FDX, spoke in support of the financial services industry moving from screen scraping to financial grade APIs.

On October 27, 2021, CFPB Director Rohit Chopra provided testimony before the U.S. House Committee on Financial Services and discussed moving away from screen scraping to open banking APIs and acknowledged the progress made by the private sector using open APIs.

On May 24, 2022, the CFPB opened a new office, the Office of Competition and Innovation. The announcement stated that "future rulemaking by the CFPB under Dodd-Frank §1033 of the Consumer Financial Protection Act will give consumers access to their own data" (emphasis added).

On March 30, 2023, the CFPB published its Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights, culminating a review process that began on October 27, 2022, when the CFPB issued its Outline of Proposals and Alternatives under Consideration (Outline) for this rulemaking.

Technology Requirements

Firms will need modern authentication and authorization technologies in place to adopt open banking and open finance, along with the appropriate technical infrastructure to support APIs at scale. The most common authentication protocol, OAuth, is available in almost all modern consent and customer identity access management platforms (CIAM). It is likely that the OpenID Foundation extension of OAuth2, known as FAPI, will be required of ecosystem participants. Open banking will typically need to align with a company's cloud strategy to obtain the appropriate scale and flexibility.

FDX Certification

The true benefits of open banking for individual banks and the financial services industry are not realized until financial APIs are interoperable. "Interoperability" refers to the ability of two pieces of software to easily connect with each other to share services and data. Interoperability is a necessary condition to enable seamless customer experiences, allow for data portability, empower rapid integration with strategic third-party partners, and help competition flourish. Data portability is a bank customer's ability to easily transfer their data from one bank, fintech app, or other data source to another party or platform. Data portability is a stated goal of the CFPB.

FDX Certification will provide regulators and industry stakeholders confidence that each certified institution's FDX APIs meet a minimum set of data, security, controls, and capabilities. This minimum set of standards will ensure interoperability and data portability that will eventually allow the financial industry to obtain the network effect.

The network effect, in the context of open banking, is a phenomenon whereby the growth of an interactive financial services community benefits both customers and providers. As the number of interconnected open banks grows, it will attract more customers and more innovative fintech partners. The network effect will benefit banks by giving them access to more potential customers and innovative strategic partners. Customers will benefit by having access to innovative products and services and data portability.

Monetization

Monetization of open finance by banks is primarily realized through customer acquisition and retention by offering premium APIs to commercial bank clients. Commercial clients can realize efficiencies by using APIs to reduce manual and semi-manual processes, e.g., the manual process of downloading transactions from a treasury management portal and subsequent upload to the client's ERP system.

Open banking APIs are quickly becoming a staple of automation and commercial customers may choose financial service providers that access these API services over providers that do not. Secondary to these commercial offerings, value is created by providing all customers additional information around spending habits and other activities using the open banking ecosystem (data into the bank).

Similarly, there are additional value drivers in the observability of customer data flowing out of the bank via APIs, such as understanding why customers use certain fintech applications. Other key activities related to consumer open banking are customer experience, risk reduction, and compliance actions, which may not directly generate revenue.

Third- and Fourth-Party Legal Agreements

The U.S. regulatory expectations for open banking are still maturing, but banks can begin to enhance consumer control over the data they share with financial applications (apps) through API-related data sharing legal agreements. Firms may also consider fourth-party relationships when forming data sharing agreements with data access platforms.

FDX Taxonomy

Consent
The permission granted by an End User to a Data Provider to authorize access to the End User's data by a Data Recipient. Consent is held by the Data Recipient to access/store/use data to provide services to the End User.

Consent API
The application programming interface that transmits Consent Scope data.

Consent Dashboard
A digital experience that enables the End User to view, edit, or revoke the Consents they have granted and the parties or processes accessing data.

Consent Grant
The act of establishing permission by an End User to a Data Provider to authorize access to the End User's data by a Data Recipient.

Consent Scope
The specification that defines what data is requested, between whom, its purpose, and duration for a specific consent granted by an End User.

Consumers
Are end users acting in their personal capacity (individuals).

Credentials
Any data used to identify the End User to the Data Provider, such as a username and password pair, to gain access to the End User's Financial Account Information.

Data Access Platforms
Intermediaries that facilitate financial data access, transit, storage and/or permissioning on behalf of Data Recipients or End Users, also commonly referred to as "data aggregators." In some cases, Data Access Platforms may not have a direct relationship with the End User. The data may be passed through without modification or may be normalized in line with permitted objectives (e.g., parsed for readability or used to confirm other data). Data Access Platforms should not be misidentified with parties who do not obtain End Users' consent but gather data, sometimes referred to as Data Brokers or Data Harvesters.

Data Brokers
Collect personal information from public and private records and provide this information to public and private sector entities for many purposes, from marketing to law enforcement and homeland security purposes. Brokers often collect and share data without end user consent (or at best rely on implied consent).

Data Cluster
A group of data elements that communicate to an End User the scope of data to be shared under a consent.

Data Harvesters
Use communication and information services, including applications (apps), to collect data from End Users and provide the data or derived digital products to third parties. Harvesters often collect and share data without end user consent (or at best rely on implied consent).

Data Providers
The entities who hold End Users' Financial

Account Information, including, without limitation to banks, credit unions and brokerages.

Data Recipients
Service companies, applications (financial apps), fintech companies, financial institutions, products, and services where End Users (on their own or through their End User Delegates) manage or act on their finances, whether actively managing their finances (such as moving money or applying for credit) or passively doing so (such as garnering recommendations or insights).

Derived Financial Data
Consists of observations, data profiles, analysis or models derived from Financial Account Information.

End User
Includes Consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data or authorize transactions with Data Recipients.

End User Authentication
Process by which the End User's access to Financial Account Information is authenticated by the Data Provider. This is accomplished via different mechanisms:

- **Legacy tech** (aka Account Credentials-based access)—the Data Access Platform or Data Recipient typically stores the End User's Account Credentials and authenticates access to accounts with the Data Provider on behalf of the End User. Such access is typically limited to Type 1 authentication factors (see authentication factors above).

- **Modern tech** (aka tokenized access)—The End User authenticates directly with the Data Provider. Note: End Users do not provide their Account Credentials to either the Data Recipient or the Data Access Platform in this model.

End User Authorization
Process by which the End Users consent to share their Financial Account Information with Data Access Platforms or Data Recipients:

- **Legacy tech** (aka Account Credentials based access)—The End Users provide their Account Credentials to the Data Recipient and/or the Data Access Platform or access to the Data Provider on behalf of the End User. The resulting Consent can only be revoked at the Data Recipient or the Data Access Platform.

- **Modern tech** (aka tokenized access)—The End Users authorize the Data Providers directly to share their Financial Account Information with the Data Recipients and/or the Data Access Platforms. In addition to consent revocation at the Data Recipient and Data Access Platform, this also permits the Data Provider to manage the End User Consent and allows the End User to revoke it at the Data Provider.

End User Delegates
Refers to delegated persons or entities,

such as End Users' CPAs, brokers, fiduciaries, and other advisors, who have been authorized by the End User to grant permission to share and receive the End Users' Financial Account Information on the End Users' behalf.

Financial Account Information
The financial accounts, statuses, histories, statements, balances, and holdings, plus transactions reflecting monetary and financial actions directly sourced from Data Providers.

Fintech
A combination of "financial technology," the word often refers to a financial technology company that offers automated tools to End Users to use their financial data.

Open Finance/Open Banking
While these terms are evolving and are often used interchangeably, they generally refer to an End User's ability to access and share their own financial data. Different terms are often linked to the presence or lack of regulation, whether they be government-regulated financial data sharing regimes, market driven systems of End User permissioned data sharing or some hybrid of the two. Other similar terms include consumer directed finance, connected banking or permissioned data sharing.

Open Banking Lead
A position created by the Canadian Government to develop a "made-in-Canada" regime based on the recommendations in the final report of the Advisory Committee on Open Banking. The Open Banking Lead will engage with industry, regulators, and consumer representatives to design and implement key pillars of the open banking system, including common rules and an accreditation framework for open banking participants.

Screen Scraping (aka Data Scraping and Web Scraping)
A method for the retrieval of Financial Account Information typically using an End User's Account Credentials (provided by End Users to a third party to obtain their Financial Account Information as though the End Users were connecting to the Data Provider). The modality of such access is often, but not limited to, from an HTML (Hypertext markup language) page via electronic means (usually via automated script) but can also be from terminal emulation, API, or another interface.

Strong Customer Authentication (SCA):
Prescribes the use of two or more of these factors, known as Multi Factor Authentication (MFA):

- **Type 1:** Something you know— passwords, PINs, code words, etc.
- **Type 2:** Something you have— typically smart phones, token devices, etc.
- **Type 3:** Something you are— Biometrics (e.g., fingerprints, facial recognition, or retina scans).

FDX Glossary and Industry Definitions

API
API stands for Application Programming Interface (API), which is an automated way of allowing two applications to talk with each other. APIs are the building blocks of open banking.

API Products
API Products are open banking APIs that are branded and sold for a fee to clients and third parties for open banking and embedded finance.

Banking-as-a-Service (BaaS)
Banking-as-a-Service is a business model by licensed banks to expand their customer reach through the open banking ecosystem. Banking-as-a-Service is a way of offering licensed bank services as white-label or cobranded services on digital marketplaces, cloud marketplaces, independent software vendors, payment facilitators, 3rd party partners, or directly to customers. With BaaS, non-bank businesses can integrate digital banking and payment services directly into their own products, software, or processes.

Buy Now, Pay Later (BNPL)
Is short-term financing, often linked to a specific purchase at the point-of-sale as an embedded finance capability, which splits a payment up into installments that the customer pays overtime.

Embedded Finance
Embedded finance is a customer experience enabled by the open banking ecosystem that occurs when a financial institution's products, services, or data appear as a digital feature within the software of a bank's customer or a third-party provider. Embedded finance features could be used in an interactive user experience or as part of an automated process.

Enterprise Resource Planning (ERP)
Systems used to manage and interpret daily business activities such as accounting, production, sales, supply chain, and workforce.

Financial Grade API (FAPI)
An API that meets the OpenID Foundation (OIDF) industry specification for banking use cases. The requirements specific data, security, privacy, and interoperability requirements for APIs. FAPI requirements for APIs are more secure than standard OAuth or Open ID Connect requirements.

Open Finance
Open Finance is an extension of open banking and can be used interchangeably. Some countries such as the UK had regulatory definitions for open banking that initially focused on data and payments. Open finance refers to additional services beyond data and payments, such as embedded point-of-sale financing, embedded foreign exchange or other products/-services that can be offered via APIs.

Optical Character Recognition (OCR)
A process for a computer to convert images of text to digital text (text that is machine-readable or searchable).

Software-as-a-Service (SaaS)
A software licensing and delivery model where software is licensed on a subscription basis and the vendor manages and hosts the software licensed to the client.

The open banking/open finance industry involves a range of financial industry participants: banks, financial institutions, financial data aggregators, fintechs, industry utilities, payment networks, consumer groups, financial industry groups, and other stakeholders involved in user-permissioned financial data sharing. While this report generally references banks and how to improve the business of banking, much of the analysis can apply to other financial industry participants whose engagement in the open finance market involves many of the same issues. Non-bank entities can learn how banks are seeking to improve their services through open finance by offering such services to banks and other industry participants. References to the U.S. market, U.S. laws, and the like, will require certain modification or analysis to confirm applicability in other jurisdictions.

The information provided herein is for educational purposes only and is not intended to be a guide for any specific company. Each company should consult with its own legal, IT, data security, financial, tax, and other advisors before implementing any programs described herein. While this report discusses certain pending regulations and policies, FDX does not endorse nor lobby for any regulatory actions or policies. Nothing herein shall be deemed an endorsement thereof. FDX intends to comply with all applicable laws and regulations related to the FDX API. Advisory statements such as "should," "plan," "implement," or other similar statements are ultimately the implementers' decisions based on their unique facts and circumstances.