Open Banking with CIBC

PROJECT PROPOSAL

Shafat Khan, Avril Rahman, Carsten Kong, Razone Rashid

TABLE OF CONTENTS

00	**Canada's Advisory Commitee**	Recommended guideline for the Open Banking System
01	**Ensure Trust**	Provide safe and reliable resources for customers
02	**Securing APIs**	Protecting data to mitigate breaches
03	**Use Case Example**	How is open banking used currently
04	**Blockchain Technology**	Blockchain technology used with Open Banking

What is Open Banking?

Allowing third party financial services to provide better customer insights to company and customer and optimize their banking functionality through the use of APIs.

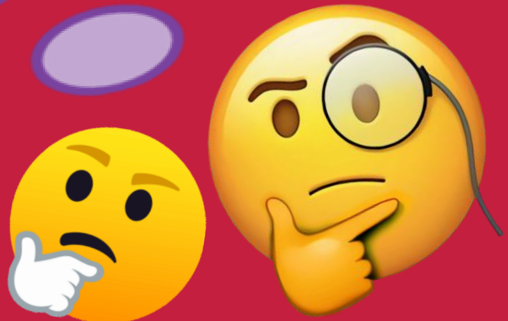
00

Canada’s Advisory Committee on Open Banking

Vision & Challenge

For CIBC to embrace the potential adoption of open banking…

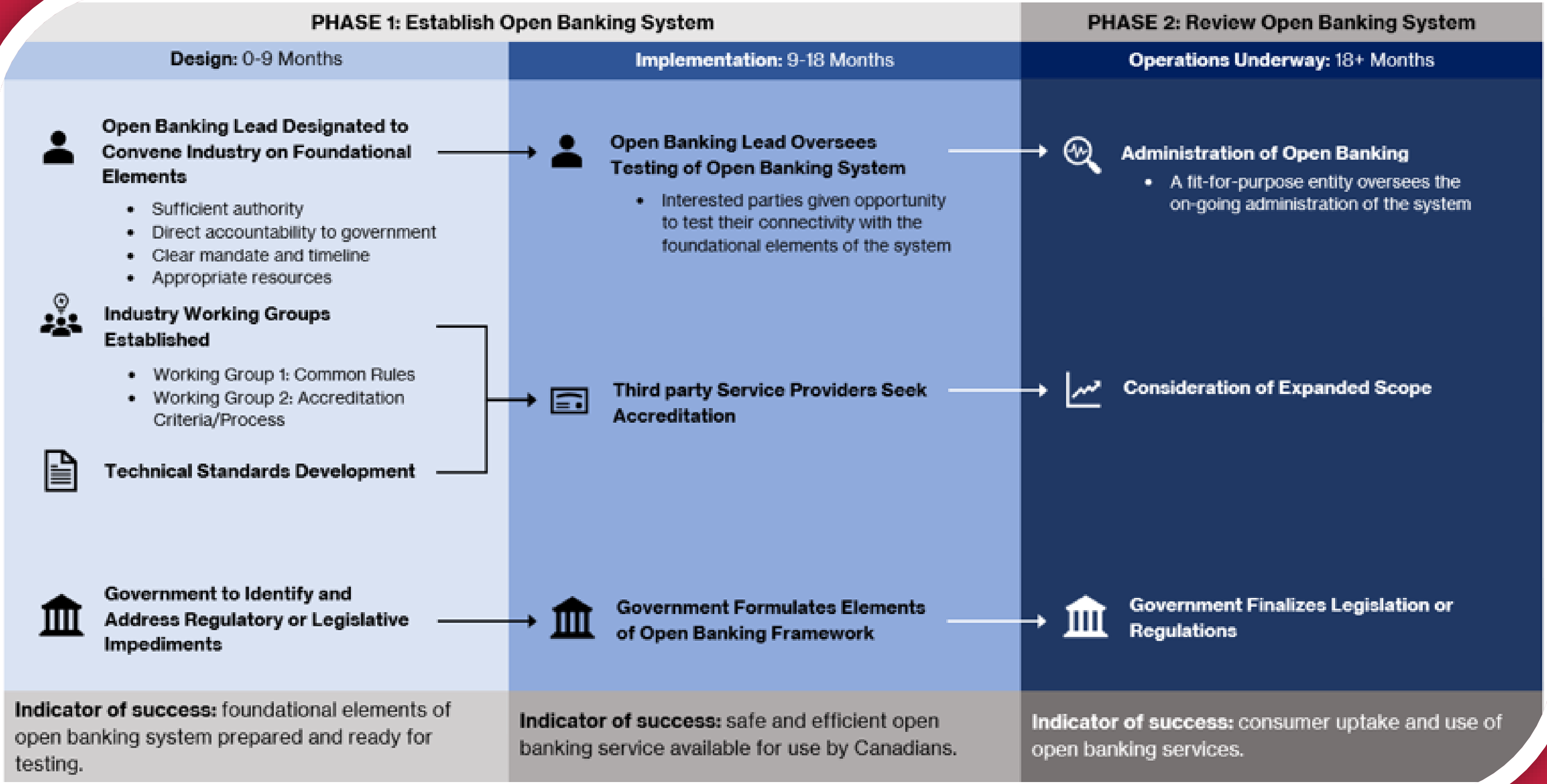
It must first consider Canada’s own vision for open banking



https://[illegible]
https://[illegible]

Advisory Committee on the Open Banking System :

Implementation Plan



PHASE 1: Establish Open Banking System

Design: 0-9 Months

Open Banking Lead Designated to Convene Industry on Foundational Elements

- Sufficient authority
- Direct accountability to government
- Clear mandate and timeline
- Appropriate resources

Industry Working Groups Established

- Working Group 1: Common Rules
- Working Group 2: Accreditation Criteria/Process

Technical Standards Development

Government to Identify and Address Regulatory or Legislative Impediments

Indicator of success: foundational elements of open banking system prepared and ready for testing.

Implementation: 9-18 Months

Open Banking Lead Oversees Testing of Open Banking System

- Interested parties given opportunity to test their connectivity with the foundational elements of the system

Third party Service Providers Seek Accreditation

Government Formulates Elements of Open Banking Framework

Indicator of success: safe and efficient open banking service available for use by Canadians.

PHASE 2: Review Open Banking System

Operations Underway: 18+ Months

Administration of Open Banking

- A fit-for-purpose entity oversees the on-going administration of the system

Consideration of Expanded Scope

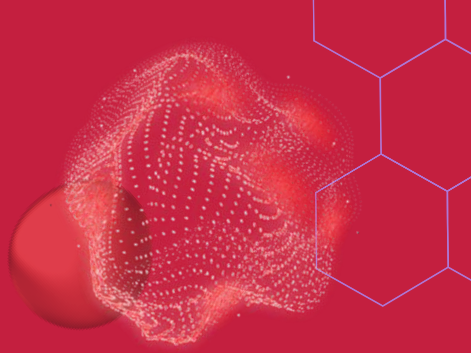
Government Finalizes Legislation or Regulations

Indicator of success: consumer uptake and use of open banking services.

Advisory Committee on the Open Banking System :

Achieving Success

- Eliminating the use of screen scraping when consumers and small businesses intentionally share their data safely and efficiently to access products and services
- Welfare of Canadian consumers and businesses is enhanced by the availability of open banking services
- Safety and stability of Canada's financial system are not compromised while supporting Canada's innovation, economic growth, and financial sector's global competitiveness



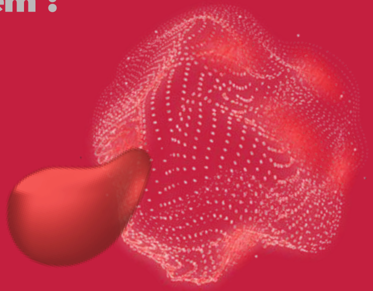
Advisory Committee on the Open Banking System :

Guideline

- The Advisory Committee recommends a hybrid, made-in-Canada approach to an open banking system that is neither exclusively a government nor industry-led model, but the best of both sectors based on currently deployed models abroad
- The Industry is recommended to manage the implementation and administration of the system, while the Government convene with participants, establishes policy objectives, and set a framework with a timeline
- The system should be capable of working with international systems of open banking

Advisory Committee on the Open Banking System :

Vision



- Consumer outcomes:
  - Their data is protected
  - Are in control of their data
  - Receive access to a large range of useful, competitive, and consumer-friendly financial services
  - Have reliable, consistent access to services
  - Have recourse when issues arise
  - Benefit from consistent consumer protection and market conduct standards
- Financial education policies, programs, and resources should be complemented by the system design

Advisory Committee on the Open Banking System :

Scope

- Participants:
  - Federally Regulated Financial Institutions (like CIBC): Required in the initial scope of the system
  - Provincial Financial Institutions: Can join voluntarily
  - Other Entities (like third-party service providers): Allowed if accreditation criteria are met, and rules of the system are followed
- Consumers and SMEs have the initial scope applied to them both
- Currently available customer and small business data from online banking applications are to be reflected in the initial scope
- The data shared by the initial scope of Canada’s open banking system should not be limited to specific use cases

Advisory Committee on the Open Banking System :

Data Scope

- Consumer-provided data, product data, balance data, transaction data, and publicly available data should be part of the initial open banking scope
- Derived data should be allowed to be excluded by financial institutions and be obligated to justify any exclusion
- Include consumer data held by third-party service providers in an open banking system and has similar exceptions for derived data
- The initial scope is to be limited to read access functions but also allow new types of data and write access functions to be expanded when all risks are fully understood and resolved
- Consumer-permissioned data mobility requests are equally required from all participants within the system
- Reciprocal data access must be granted through express consumer consent, and cannot be demanded from consumers to receive a participant’s product or service

Advisory Committee on the Open Banking System :

Governance

- Governance of the system will proceed in a phased approach to scale with the risk associated with the system
- Must be transparent, impartial, and representative of all parties in the system
- Key elements needed to be addressed before the system can begin operating in the country: Common rules, An Accreditation Framework, and Technical Specifications
- Responsibility of the Government:
  - Oversee the entire process of the implementation plan
  - Ensure consumer representatives are involved in the process
  - A formal governance entity established to provide administration and transition to an open banking system following the conclusion of the lead’s work program
  - Formally codify elements of open banking in legislation or regulation, and add additional functions or products over time

Advisory Committee on the Open Banking System :

Common Rules

- Established to ensure a system is efficiently functioning to protect consumers and guarantee a positive consumer experience
- Ensures consistent and high standards of consumer protection safeguarding the transmission of data while avoiding regulatory overlap in how data is used
- Articulate that liability flows with data and falls to the party at fault
- Ensures every participant must have mechanisms in place to handle internal and external complaints and data traceability protocols
- Prescribes clear and automatic terms of redress for consumers such as immediate compensation for any financial loss, following appropriate standards of care for protection, and remedying a loss of sensitive financial data
- Rules surrounding privacy focus on two areas: Consent Management and Privacy Management
- Prohibit undue pressure on consumers and ensure that information given to consumers is accurate, clear, and not misleading while requiring public disclosure for consumer complaints received

Advisory Committee on the Open Banking System :

Common Rules (Cont.)

- Security must be developed in the areas of:
  - Data Security: includes Authentication, authorization, access management, data transit and encryption, tokenization, auditability, and traceability
  - Operational & Systemic Risk: includes APIs security & technical standards that include prevention, IT security infrastructure, incident response & monitoring, penetration testing, and recovery measures
- For entities pursuing accreditation with stronger security standards required based on risk, a minimum "floor" of security standards must be followed
- Development of educational tools/resources are required to raise consumer awareness of their rights and responsibilities should

Advisory Committee on the Open Banking System :

Accreditation

- Sufficiently robust accreditation criteria to protect consumers without excluding a wide range of market participants
- Sufficient criteria to demonstrate that participants can comply with common rules related to liability, privacy, and security, with the sufficient financial capacity to ensure consumer protection in the event of loss
- The process of accreditation must be trusted, transparent, independent, proportional to risk, and coherent with other regulatory regimes
- Consumers and other market participants must be able to access the accreditation criteria and the list of accredited firms easily
- Firms will bear the cost of the accreditation process when seeking accreditation with a party outside the open banking system

Advisory Committee on the Open Banking System :

Technical Specification & Standards

- Must be accessible ad inclusive for all accredited system participants without needing additional requirements
- Allow a positive consumer experience without needing complex steps for consumers to follow to understand the benefits of open banking
- Ensures safe and efficient transfer of data among system participants
- Can adapt to technological change to keep pace with the consistently changing sector
- Flexible with the development of new and innovative products
- Capable of working with international approaches to open banking

01

How Do We Ensure Trust

Use of Privacy Principles

Adopt Privacy Principles

- Control: Giving customers the authority and understanding of where their data is going and how they can access their data (Provide correct tools and clarity)

- Transparency: What is required from the customer, Why is it required, What is its purpose

- Security: Authorization and Authentication clarity between bank, 3rd party API, and customer. Who has your data, what is the data being used for. Emphasize protection to customers to make them feel safe when using 3rd party APIs

- Legal Protection: GDPR

- Benefits for Users: Giving the best user experience with API design, clarity and accessibility to the users' real-time data

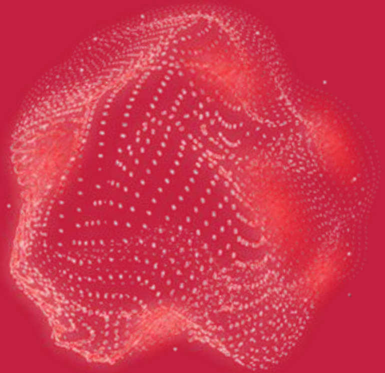
Operation Standards for APIs

- Leverage API management tools and gateways
- Support older versions of API
  - Notify users if a specific version of API will not be usable before launching
- Authenticate Appropriately
  - Strong authentication and authorization protocols (OAuth, MFA)
  - Rate limiting - don’t overuse resources
  - Enabling specific users with their appropriate amount of access
- Monitoring and Logging
  - Leverage SIEM/SOAR for unusual behaviour
  - When was data access, by whom
  - *Falco* detects anomalies within cloud and containers, detects when API key is made
- Data Protection
  - Use of encryption, hashing and tokenization

Implementing & Benefits of APIs

- Banks should ensure APIs are secure and compliant with regulations
- Banks should partner with third-party developers to ensure APIs are up to date with the latest technologies and trends

- Saves cost
- Improves customer service
- Improves industry-level collaboration
- Gather data for business intelligence
- Creates new revenue models



02

How Can We Secure APIs

Threats & Solutions

3rd Party Risks

- Security Risks:
  - Expose sensitive financial data to other providers
- Privacy Risks:
  - Providers may collect customer data which are not in accordance with customer preferences
- Operational Risks
  - May experience in service disruption or data breach

Potential Threats

- Coding Bugs: Coding Errors
- Injection Attacks: XXS Attacks, SQL Injections
- Availability Threats: DDoS Attacks
- User Identity Threats: Fraudulent Activity
- Insider Threats

Threat Resolution

- Reviewing code and testing constantly via CI/CD pipelines
  - Engage 3rd party penetration tests

- Consistent Input Validation:
  - Checks consistency of node instances
  - Use API management platform to assist with input validation
  - Helps protect against injection attacks

- Implement access controls

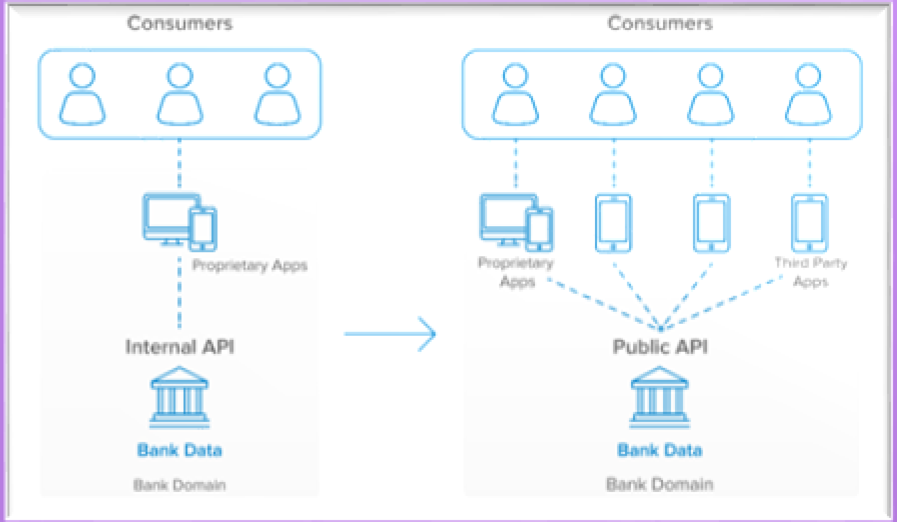
- Integrate SSO (Single sign-on) with API management

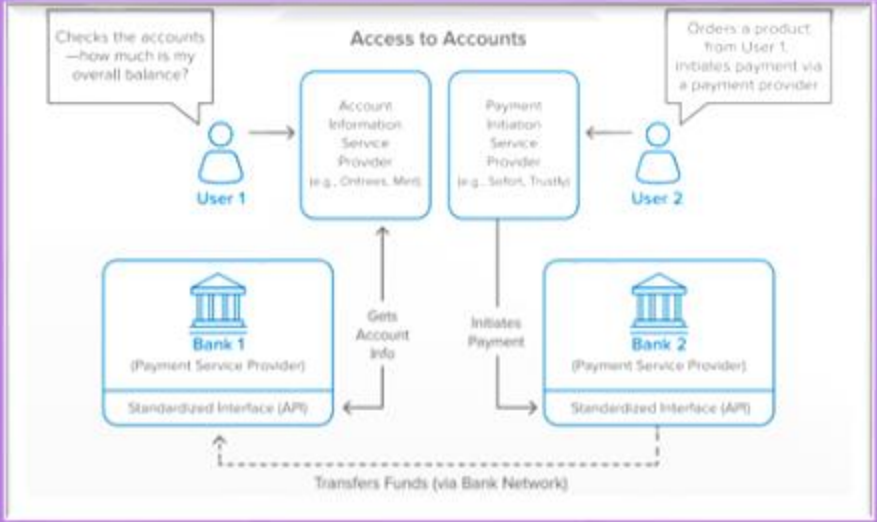
- Encrypt requests and responses

- Validate data

- Authenticate and authorize (Using OAuth framework)

PSD2 (Second Payment Services Directive) Regulations




Checks the accounts —how much is my overall balance?
Access to Accounts
Orders a product from User 1, initiates payment via a payment provider
User 1
Account Information Service Provider (e.g., Ontrees, Mint)
Payment Initiation Service Provider (e.g., Sofort, Trustly)
User 2
Bank 1
(Payment Service Provider)
Standardized Interface (API)
Gets Account Info
Initiates Payment
Bank 2
(Payment Service Provider)
Standardized Interface (API)
Transfers Funds (via Bank Network)

03

Open Banking Use Case

Real Life API Implementation

× Tink ×

- Europe's leading open banking platform.
- With one API it allows users to:
    - Access aggregated financial data
    - Initiate payments
    - Verify account ownership
    - Build finance management tools

Affordability assessment

Simplified with Tink.

How Tink's API Works

Aggregating

- Fetches transaction data from 3,400+ financial institutions in Europe
- API gives a more detailed view of user's finances then a credit check

Meaningful Data

- Aggregated data is refined which allows Tink to understand one's spending habits
- Made possible by their scalable self-learning machine model

Real-Time

- Refined data is fed to your credit scoring risk model, It enables users to:
    - Make better risk assessments
    - Informed credit decisions

What Makes the API Safe?

- Encryption
  - Protects data at rest and in transit
- Authentication
  - Users must obtain access token from Tink
- Monitoring
  - Monitors and logs all activity and requests
- Vulnerability testing
  - Performs security assessments and penetration testing
- Strict compliance regulations

04

Open Banking X Blockchain Technology

Smart Contracts

Programs stored on a blockchain that run when predetermined conditions are met. No trust required

× Implement Smart Contracts With API's

Give API's predetermined conditions to execute

× Permissions

Give the API the required permissions to run its tasks and access accounts

× Multifactor Authentication

Ensures that only authorized users can access the API, also enables the API to enter accounts

Additional Key Considerations

UX/Design

- Increases competition in the financial industry, leads to better, innovative and more friendly financial products/services for consumers
- Easier for consumers to manage their money and compare different financial products/services
- Solution: Provide a sandbox tutorial of the experience towards a specific API

Cloud/Data/AI

- Boost digitization processes through its unified storage and metadata capabilities
- AI helps banks to process large volumes of data and predict the latest market trends, currencies, and stocks

Information Links

- Final Report - Advisory Committee on Open Banking
- What is Tink?
- Tinks Tech
- What are Smart Contracts?
- Protect API in Azure API Management using OAuth
- How to Prevent a DDoS Attack
- What open banking means for Canada's financial landscape - PWC
- API Technical and data standards
- Customer Experience Principles – Open Banking
- UX/UI Guides On How To Increase Open Banking Adoption
- Cloud Computing as an enabler of Open Banking

Thank You!

DO YOU HAVE ANY QUESTIONS?