# The Balancing Act: Open Banking

Spring Academy: Privacy + Security Forum
May 9. 2024



We're all connected.

LOEB & LOEB LLP

LOS ANGELES
NEW YORK
CHICAGO
NASHVILLE
WASHINGTON, DC
SAN FRANCISCO
BEIJING
HONG KONG

loeb.com

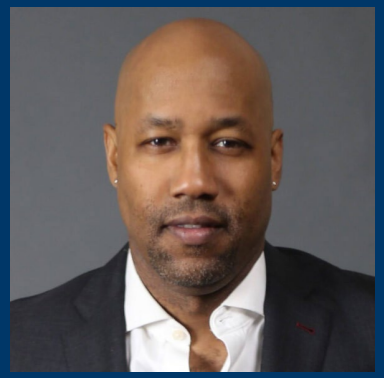
The opinions expressed in this presentation do not necessarily reflect the views of Loeb & Loeb LLP, its clients or the Panel Members respective companies. This document was created for purposes of guiding the presentation discussion, and should not be posted to the Internet, or otherwise used for any commercial purposes, without prior written approval from Loeb & Loeb LLP. The information in this document is not intended to be and should not be taken as legal advice.

# Speakers

Eyvonne Mallett
Of Counsel
**Loeb & Loeb**

Bianca Lewis
Associate
**Loeb & Loeb**

Jolevette Mitchell
Vice President and Senior Counsel
**Apple Bank**



Jacques Sexton
Assistant General Counsel, Privacy, Legal & Compliance
**DailyPay**

# Agenda

- Background
- What is the Open Banking Rule?
- Who is Covered by the Open Banking Rule?
- Requirements for Data Providers
- Requirements for Third Parties and Data Aggregators
- Privacy and Security Challenges
- Best Practices

# Background

In 2010, Congress included in the Consumer Financial Protection Act (CFPA) Section 1033 requiring that the Consumer Financial Protection Bureau (CFPB or Bureau) promulgate rules effectuating what is commonly referred to as “Open Banking.”

- Section 1033’s proposed rule requires any entity that engages in offering or providing a consumer financial product or service to make available information concerning the financial products or services that the consumer received from the entity
- In October 2023, the CFPB issued a proposed rule to implement the CFPA’s open banking/consumer financial data right under Section 1033
- The public comment period for the proposed rule closed on December 29, 2023, but the rule has yet to be finalized

# What is Open Banking?

# What is the Open Banking?

The open banking rule will give consumers the ability to share financial accounts' data with third parties — either a different financial institution than the consumers primary bank or third party. These third-party providers can include a wide range of fintechs, currency exchanges, merchants and other digital platforms.

Sharing bank account data with another financial services provider may unlock new or improved financial services — most often via apps — including those that make it easier to access credit and manage money in one seamless interaction.

# Who is Covered by CFPB's Open Banking Rule?

# Who is Covered by the Open Banking Rule?

## Three Primary Actors in the Open Banking Ecosystem

*Data providers*

Card issuers, financial institutions, or other entities that control or possess information concerning a covered consumer financial product or service that the consumer obtained from the data provider.

*Data Aggregators*

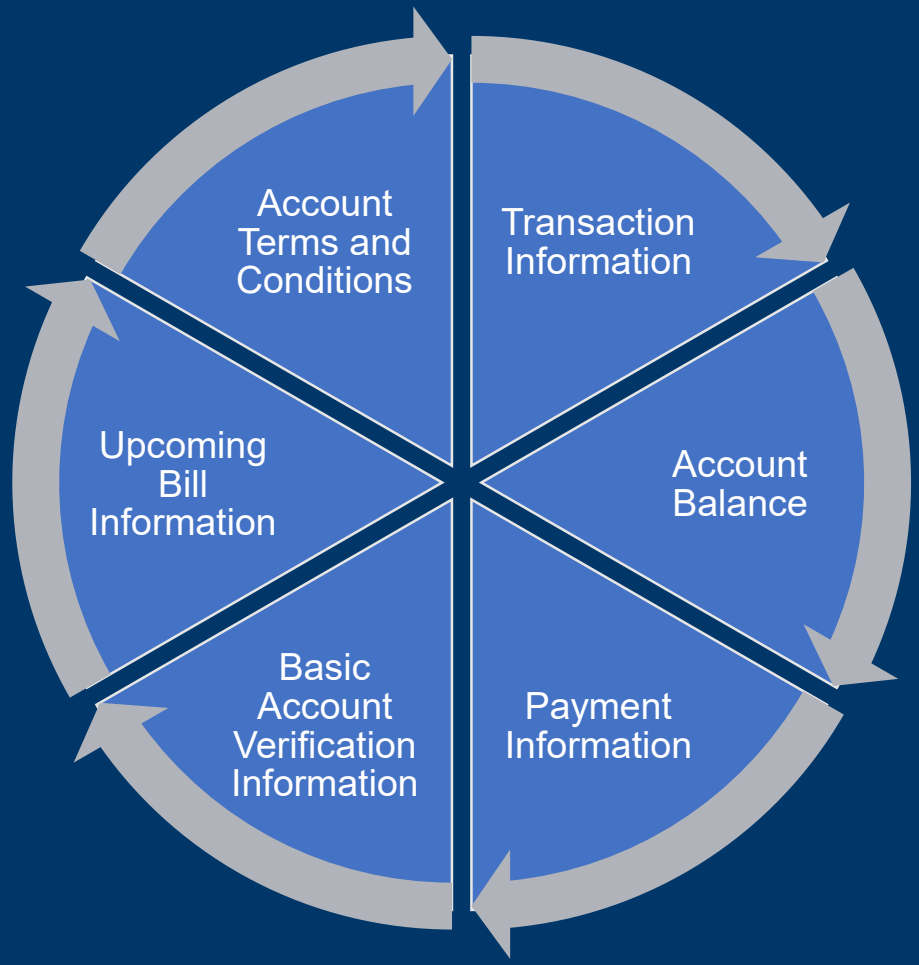
*E*ntities that are retained by authorized third parties as service providers to assist with accessing covered data on behalf of a consumer.

*Authorized third parties*

Third parties that have satisfied the authorization requirements under the Proposed Rule and are thus permitted to access covered data on behalf of a consumer.

# Requirements for Data Providers

# Requirements for Data Providers: Sharing Various Types of Financial Information



# Requirements for Data Providers: Prohibitions on Sharing Certain Information

- Data providers are not required to make available:

(i) confidential commercial information, including algorithms used to derive credit scores or other types of risk scores;

(ii) information collected for the sole purpose of preventing fraud or money laundering, or for detecting or reporting other potentially unlawful conduct;

(iii) information required to be kept confidential under other applicable law, provided that the exception does not apply to the consumer's own information merely because it is subject to privacy protections; or

(iv) information that is not retrievable in the ordinary course of business.

# Requirements for Data Providers: How Must the Data Be Provided?

Data providers are required both to:

1. maintain consumer interfaces (e.g., online banking), and
2. establish and maintain developer interfaces (e.g., application programming interfaces (APIs)) through which the data provider receives and responds to requests from authorized third parties.

For specific requests, data providers must also make available machine-readable files containing covered data suitable for loading into a consumer or an authorized third party's own systems. Data providers are prohibited from charging fees to either consumers or authorized third parties to access the interfaces.

# Requirements for Third Parties and Data Aggregators

# Requirements for Third Parties and Data Aggregators

- Third party must obtain a consumer's authorization. The authorization must be clear and conspicuous and be separate from other materials or terms.
- If a third party uses a data aggregator, the data aggregator may provide consumers with the authorization notices and obtain consumer's express consents on behalf of the third party. The data aggregator would need to provide its own certification to the consumer regarding compliance with the rule and the restrictions on the collection, use, and disclosure of the consumer's covered data. The third party would still be responsible for complying with the rule's authorization requirements.
- A consumer's authorization, unless revoked earlier, would remain in effect for 12 months.
- A third party may only collect, use, and disclose covered data as reasonably necessary to provide a specific product or service that a consumer requested.
- Open Banking data is prohibited from being used for any secondary purposes, and the proposal expressly prohibits collecting, using, or disclosing covered data for targeted advertising purposes, to cross-sell other products or services, or for any sale of covered data.

# Requirements for Third Parties and Data Aggregators

- Authorized third parties are subject to a number of obligations related to their access to covered data on behalf of a consumer, including:
  - Restrictions on collection, use and retention
  - Requirements to ensure data accuracy
  - Information security requirements
  - Communication requirements
  - Revocation requirements

# Privacy and Security Challenges

## Privacy

- Data Consent
- Data Control
- Data Minimization
- Data Retention
- Transparency

## Security

- Authentication
- Authorization
- Potential for Data Breaches
- API Security
- Third Party Concerns (Vendor Management)

# Closing Insights

What advice or tips do you have for developing an open banking program that mitigates privacy and security challenges?

# Tips to Address Privacy and Security Challenges

| | |
|---|---|
| **Strong Authentication** | • Implementing multi-factor authentication, biometric authentication, or token-based authentication can improve the security of client accounts and APIs. |
| **Secure API Design and Implementation** | • Developing secure APIs with sufficient input validation, access controls, and encryption helps reduce the risk of API-related vulnerabilities. |
| Data Encryption | • Encrypting sensitive data at rest and in transit ensures that even if data is intercepted or compromised, it remains unintelligible and unusable to unauthorized parties. |

# Tips to Address Privacy and Security Challenges

| | |
|---|---|
| **Privacy by Design** | • Implementing privacy-enhancing technologies and techniques such as pseudonymization, anonymization, and data minimization can preserve consumer privacy and ensure that only relevant data is transmitted. |
| **Regulatory Compliance** | • Financial institutions and third-party suppliers must follow appropriate legislation, such as the Gramm-Leach-Bliley Act or local data protection laws, to secure the privacy and security of consumer data. |
| **Enhancing and Privacy in Open banking through Blockchain Technology** | • Blockchain technology provides a decentralized and immutable ledger where data can be securely stored and accessed. In open banking, where sensitive financial data is shared among multiple parties, the immutability of blockchain records ensures that once data is recorded, it cannot be altered or tampered with. |

# QUESTIONS?