

CFPB's Open Banking Proposal

Understanding the Potential Impact on Stakeholders and Promises and Pitfalls for Innovative Loan Underwriting

Jeffrey P. Taft

Partner – (202) 263-3293
jtaft@mayerbrown.com

Eric T. Mitzenmacher

Partner – (202) 263-3317
emitzenmacher@mayerbrown.com

February 14, 2024

Kelly F. Truesdale

Associate – (202) 263-3294
ktruesdale@mayerbrown.com

1

Section 1033

- Section 1033 of the Dodd-Frank Act

Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.

- Largely dormant authority, although the CFPB had taken some steps in recent years, e.g., information requests and an ANPRM
- On October 19, 2023, the CFPB released the Proposed Rule

2

2

Historical Context

- Pre-Dodd-Frank Rationale for Consumer Data Portability
 - Competition — Portable data would mitigate a significant barrier to entry for new entrants, and force established players to compete
 - Innovation — Broader access to data + more competition + increasing technological sophistication → new or better consumer financial products and services
 - Security — Early attempts at aggregation involved password sharing and screen scraping, creating tension between benefits of broader access to data and traditional information security and consumer privacy concepts
 - Politics — A large percentage of consumers just wanted it

3

MAYER | BROWN

3

Historical Context (cont.)

- Section 1033 did not draw much attention in legislative process
- Dodd-Frank was not first attempt to address account aggregation
 - “Bank-Provided Account Aggregation Services” - OCC Bulletin 2001-12 (Feb. 28, 2001)
 - “Foreign-Based Third-Party Service Providers” - OCC Bulletin 2002-16 (May 15, 2002)
- Market shifts in access to consumer data since Dodd-Frank and increased focus on privacy, cybersecurity, AI and information brokers
- CFPB focus on competition as way of fighting higher fees and this rulemaking fits into large initiative

4

MAYER | BROWN

4

Personal Financial Data Ecosystem Participants

- Data providers
 - Entities that control or possess information concerning a covered *consumer financial product or service* that the consumer obtained from the data provider
- Authorized third parties
 - Third parties that have satisfied the authorization requirements to access covered data on behalf of a consumer
- Data aggregators
 - Entities retained by authorized third parties as service providers to assist with accessing covered data on behalf of a consumer

5

MAYER | BROWN

5

Covered Financial Products & Services

- Three initial consumer financial products or services
 - Regulation E accounts
 - Regulation Z credit cards
 - Payment facilitation services from a Regulation E account or Regulation Z credit card
- The CFPB has indicated that it intends to extend coverage to other consumer financial products and services

6

MAYER | BROWN

6

Basic Covered Data

- Transaction information, including at least two years of historical transaction information
- The consumer's account balance
- Information to initiate payment to or from a Regulation E account
- Terms and conditions of the account (e.g., fees, APY/APR, OD coverage)
- Upcoming bill information (both with the provider and third-party)
- Basic account verification information, i.e., name, address, email address, and phone number

7

MAYER | BROWN

7

Methods of Accessing Covered Data

- Proposed Rule requires data providers to establish and maintain separate consumer interfaces and developer interfaces
 - Interfaces cannot share the same access credentials
 - Interfaces based on screen scraping are not permitted
- Developer interfaces (i.e., APIs) provide standardized access to covered data and must meet minimum performance, reliability and security requirements
- No fees are permitted for either consumers or authorized third parties to access the consumer or developer interfaces

8

MAYER | BROWN

8

Authorized Third Parties: Authorization

- Must obtain “express informed consent” of consumer with signed authorization disclosure providing
 - The names of the third party and the data provider for which access is sought;
 - A description of the service to be provided by the third party, and the categories of data that will be accessed;
 - A certification that the third party will comply with specific obligations related to collection, use and retention of data, access to data, data accuracy, and data security; and
 - A description of the process through which the customer can revoke the third party’s access.

9

MAYER | BROWN

9

Authorized Third Parties: Authorization

- Authorization disclosure must be clear, conspicuous and separate
- Authorizations must be renewed annually or expire automatically
- Authorized third parties must make available up-to-date information on authorization status to a consumer
- Authorizations must be easily revocable, and authorized third parties must honor revocations and inform data provider and other recipients of data

10

MAYER | BROWN

10

Authorized Third Parties: Limitations

- Must limit collection, use and retention of covered data to only what is reasonably necessary to provide the requested product or service
 - Particularly, using covered data for targeted advertising or cross-selling, and from selling covered data is prohibited
 - Must not use or retain covered data after expiration or revocation of authorization
- Must maintain policies and procedures to ensure data accuracy
- Must ensure systems for collection, use or retention of covered data are covered by satisfactory information security program

Relationship to Other Laws

- Proposed Rule has broader impact on other areas of the law
 - State and federal privacy laws
 - Information security including GLB Act safeguarding rules
 - Fair Credit Reporting Act
 - Fraud prevention services

Opportunities

Data Aggregators / Facilitators

- Significantly lower barriers to entry
- Clear and consistent data coverage and performance standards
- Opportunities for integration and specialization

Fintech Service Providers

- Commercial opportunities given that tech efficiency and big data approaches tend to be comparative advantages over traditional financial services providers
- Cross-cutting/dependent on core service set

Lenders

- Greater access to information for underwriting
- Greater ability to cross-sell consumers
- Potential for use in model tailoring and portfolio analysis, but questions remain

Secondary Market Participants

- What are the potential impacts on lenders and other financing sources as well as investors?
- Does the rule provide enough clarity for third party to evaluate potential liabilities?

13

MAYER | BROWN

13

Challenges Presented by the Proposed Rule

- API Development
 - Lack of clarity on industry standards; short development timeframe
 - Complexity of data use restrictions, authorization management
- Navigating shift from limited contracted data recipients to broad availability → potentially significant access management burden
- Ensuring that consumer data is adequately protected throughout the course of transfers and access and holding parties responsible for failure to safeguard the data
- State and federal data privacy laws and sectoral approach at federal level present challenges

14

MAYER | BROWN

14

Allocation of Risks Under the Proposed Rule

Stakeholder Perspectives

- Proper allocation of potential liability of banks and others sharing customer information in compliance with the requirements.
- Will banks bear the risk of customer fraud and other errors within the ecosystem?

Consumer Perspective

- Proliferation of companies and apps with data access provides more opportunities for bad actors, other data loss
- Uncertainty on protections around payment initiation information
- Transition from screen scraping, authorization requirements and use limitations increase protections
- Ultimately, consumer protection will depend on practical reality of implementation and enforcement

15

MAYER | BROWN

15

Disclaimer

- These materials are provided by Mayer Brown and reflect information as of the date of presentation.
- The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.
- You may not copy or modify the materials or use them for any purpose without our express prior written permission.

16

MAYER | BROWN

16

Americas | Asia | EMEA

mayerbrown.com

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) and non-legal service providers, which provide consultancy services (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong & Nair, LLC ("PKWN") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong & Nair Pte. Ltd. Details of the individual Mayer Brown Practices and PKWN can be found in the Legal Notices section of our website. © Mayer Brown. All rights reserved.