



OPEN BANKING UNLEASHED

NAVIGATING THE NEW ERA OF OPEN BANKING AND CONSUMER DATA RIGHTS



by **John Eden** | Counsel

INTRODUCTION

We wish to inform you about a significant regulatory development that could reshape the fintech landscape. The Consumer Financial Protection Bureau (“CFPB”) recently proposed the Personal Financial Data Rights (the “Proposed Rule”) rule with the intention of making consumers’ financial transaction data more portable, thereby causing a broader shift to a more open banking ecosystem characterized by increased competition between banking service providers.

SCOPE AND OPERATING OF THE PROPOSED RULE

The Proposed Rule was announced on October 19, 2023. The new rule implements section 1033 of the Consumer Financial Protection Act of 2010 (“CFPA”), a critical piece of legislation designed to ensure that markets for financial products are fair, transparent, and competitive.

This new rule applies to data providers, which include financial institutions that offer checking accounts, prepaid accounts, digital wallets, and credit cards (“Data Providers”).

The Proposed Rule implements the CFPA by imposing the following requirements on Data Providers:

- **Data Sharing:** The Proposed Rule mandates that Data Providers permit customers to share comprehensive transactional and personal information with third-party entities. This includes historical transaction data, account balances, information required to initiate a payment, basic identity information, and more (the “Covered Data”).
- **Consumer Interface Access:** The current version of the rule requires Data Providers to make Covered Data available directly to consumers through consumer interfaces that support the export of such data through machine-readable formats. Note that Data Providers who do not provide a consumer interface would be exempt from the Proposed Rule.



- **Technical Requirements for Data Sharing:** Data Providers are required to ensure that transactional data for the previous twelve (12) months is available for sharing with third parties designated by a customer.
- **Technology Development for Data Sharing Technology:**
 - The data sharing responsibilities of covered providers must be executed via secure application programming interfaces (“APIs”) that are built to support a minimum uptime of 99.5%.
 - These APIs must be developed with funding provided by the covered Data Providers themselves, and API calls must be free to fintech companies who use them.

NEW RESTRICTIONS ON FINTECH COMPANIES

- **Disclosure of Data Usage Policies:** The fintech companies that benefit from the Proposed Rule will need to disclose their data usage policies to consumers.
- **Strict Opt-In Requirements:** Fintech firms are required to disclose data use practices to consumers. They are also prohibited from using shared data for advertising, resale, or cross-selling purposes without express consent from the consumer.
- **Reliance on Bank-Provided APIs:** Covered Data must be obtained through bank-provided APIs. This will require fintech companies to work with the specific APIs utilized by the different Data Providers they interface with, potentially increasing costs and operational complexity.
- **Proscription on Screen Scraping:** In light of the broad degree of access that consumers will have to Covered Data under the proposed rule, fintech companies will no longer be permitted to engage in screen scraping. This prohibition extends to situations in which Covered Data is temporarily not available via a bank-provided API.

THE BROADER IMPACT OF THE PROPOSED RULE

The Proposed Rule would have the following short- and long-term impacts:

- **Enhanced Consumer Choice:** After the Proposed Rule is implemented, switching between banking providers will be easier because consumers’ financial data will be fully portable, thereby making it easier to find and adopt new products and services. (However, note that increased portability of financial data does not necessarily mean that new financial technology companies will spring up immediately to provide an array of genuinely new services to consumers. New startups will certainly need time to evaluate the opportunities that the Proposed Rule opens up for them to offer new services to banking customers.)




- **Open Banking and Increased Competition:**
 - Open banking emphasizes consumer ownership of financial data, facilitating its sharing without burdensome fees or undue delays from banks.
 - Banks today exert a significant amount of control over access to the financial data of their customers. The Proposed Rule loosens that control significantly, which could lead directly to reduced switching costs for consumers who want to try new products and services. If such switching cost savings materialize, the financial services sector will become more competitive.
- **Potential Increased Incentives for Innovation at Large Banks:**
 - The Proposed Rule will also place pressure on traditional banking institutions to develop innovative products in-house to respond to the increasing competition from younger fintech companies.
 - Where consumers have increased choice and lowered switching costs, traditional banking providers will naturally look for ways to delight and surprise those consumers.
 - Notwithstanding the above, Data Providers may in certain cases have existing resource and talent constraints which make the development of new products and services challenging.

POTENTIAL RISKS FOR DATA PROVIDERS

From an information security and data integrity point of view, the Proposed Rule should reduce certain types of financial fraud that are common today, particularly fraud that is carried out by exploiting weaknesses in the way we share, store, and protect online banking credentials. A world in which consumers no longer share such login credentials with a range of fintech companies should result in a non-trivial reduction in financial fraud. For example, phishing attacks will be harder to execute because Data Providers will be (1) receiving data sharing authorization requests directly from their banking customers and (2) managing the execution of those requests via APIs they control and maintain. That is very different from what happens today. At present, fintech companies often require that consumers share their login credentials (often saving those credentials for future use), a practice that makes it easy for those credentials to fall into the wrong hands.

Notwithstanding this expected reduction in certain types of financial fraud, once the Proposed Rule becomes effective Data Providers may wind up with increased levels of legal liability for the following reasons:

- Currently, customers who use fintech products and services (which have been granted access to information housed by Data Providers through data access solutions (each a “Third Party API”, collectively “Third Party APIs”) that those fintech companies have built) may find it difficult to argue that Data Providers are liable in situations where fraudulent transfers or data theft occurs as a result of actions taken by fintech companies.
- Today this argument is difficult to make because customers are responsible for authorizing third-party



financial technology companies to use Third Party APIs to access otherwise private and secure financial data held by Data Providers. The argument can always be made that in making such choices consumers assume the associated risks.

- Because banks cannot prevent customers from using a Third Party API, nor are banks responsible for the way fintech companies collect, store, and use customer data, a related argument can be made that banks are not responsible for assuming the associated risks.
- When the Proposed Rule is finalized and enforced, all of this will change for the following reasons:
 - Screen scraping and other forms of third-party access will be prohibited, as data transfers will only be authorized by way of APIs engineered and maintained by Data Providers.
 - As a result, Data Providers – not fintech companies – will have direct control over how customer data is shared with third parties.
 - That direct control over the sharing of customer data will increase the risk profile for Data Providers. When fraud and data theft occur after the Proposed Rule becomes effective, customers of Data Providers will have an easier time arguing that the party who engineered the data transfer technology – i.e., the Data Provider – should be responsible for restitution, along with any other appropriate damages.

CFPB REQUESTS FOR COMMENTS

The Proposed Rule's open comment period closed on December 29, 2023. Six months after the final rule is published, the largest Data Providers are expected to start complying with the rule's requirements (i.e., institutions with more than \$500 billion in total assets and at least \$10 billion in annual revenue).

There will, however, be a tiered compliance timeline that provides smaller depository institutions with additional time. For example, institutions that hold less than \$850 million in total assets will receive up to four (4) years to comply with the final rule.

The Proposed Rule signifies a milestone in consumer financial data rights, emphasizing data accessibility, open banking, and increased competition in the fintech sector. We recommend that traditional banking institutions, fintech companies, and related stakeholders closely monitor this evolving regulatory landscape.

Our team can help you prepare to adapt to the short- and long-term impacts of this new shift to open banking. For further information or assistance, please do not hesitate to contact John Eden (jeden@burghergray.com) or Gopal Burgher (gburgher@burghergray.com).



1350 Broadway | Suite 1510
New York, NY 10018
T: 646.513.3231 | F: 646.561.9866
info@burghergray.com