Hashed & Salted | A Privacy and Data Security Update
September 2022

CFPB's Open Banking Rule Delayed by Data Privacy and Security Concerns

The Consumer Financial Protection Bureau (CFPB) is working on a final proposal for its open banking rule. If codified, the open banking rule will enable consumers to own, access and share their financial data however and with whomever they choose. Open banking generally refers to a consumer's ability to control their financial data by allowing third-party financial service providers to access financial data in real time through the use of application program interfaces (APIs). Congress first addressed open banking through Section 1033 of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act by authorizing the CFPB to help ensure that consumers have access to the information in their financial records and the ability to leverage that data to achieve three key objectives:

- Improve competition and consumer choice
- Strengthen consumer privacy and control
- Expand financial inclusion

Yet, movement toward issuing the open banking rule has been relatively slow. Since 2010, the CFPB has published principles for consumer-authorized access and use of consumer financial information, obtained consumer and industry opinions on the developing market for consumer-authorized financial data sharing, issued an advance notice of rulemaking for the open banking rule, and added the open banking rule to the CFPB's 2022 regulatory agenda (likely prompted by President Joe Biden including open banking as one of 72 policy initiatives included in the July 2021 executive order on competition). Over the past year, the CFPB has received more than 100 public comments on the proposed open banking rule.

And recently, CFPB Director Rohit Chopra, through testimony before the Senate Committee on Banking, Housing and Urban Affairs, reiterated that open banking is a priority for the CFPB.

This begs the question: Why has one of CFPB's key priorities been delayed for over a decade?

The answer is that the inherent openness of open banking has caused financial institutions and regulators to raise data privacy and security concerns. Generally, financial institutions and regulators do not oppose the rule, but there is a common concern that open banking could put consumers' data at risk because financial technology (fintech) companies or other third-party providers may not have the same rigorous cybersecurity and privacy standards as traditional firms. As a result, in proposing a final rule, the CFPB must strike the right balance between protecting data privacy and security, allowing consumers effective control over their data, and advancing competition. In May 2022, Reuters reported that a CFPB agency source stated that the CFPB "feels the pinch" to move forward with the open banking rule but is experiencing challenges to "strik[ing] the right balance."

Attorney Advertising

Privacy and Data Security Concerns

Despite the numerous benefits of open banking, it poses an inherent risk that consumer financial data could be misappropriated or accessed by cybercriminals. In light of several recent high-profile cyberattacks in the financial services space, the protection of sensitive personal information is one of the primary concerns in finalizing the open banking rule. To put this in context, in 2021, consumers lost almost $52 billion to traditional identity fraud and identity fraud scams, with nearly $7 billion attributed to new account fraud. Unfortunately, the current patchwork of regulations and consumer protection laws does not provide a high degree of comfort regarding the protection of sensitive personal information, especially when third-party providers, included in the mix to facilitate a function such as open banking, are not directly responsible for compliance. The addition of third-party APIs makes the task of keeping data safe and secure extremely complex and outside the control of financial institutions. The frequency of identity-based attacks coupled with the lack of data exchange standards in open banking has created uneasiness among financial institutions and regulators; inconsistent data standards may increase the threats to data privacy through third-party data sharing, application fraud or security breaches, which could potentially harm both the consumer and financial institutions.

To address identity fraud and protect sensitive information, the majority of third-party providers are adopting APIs to seamlessly interface with consumers and financial institutions, but data security concerns remain. While open banking APIs allow easy access to consumer data, consumers may find it hard to keep track of who has access to their data. APIs are also a common attack vector used by cybercriminals. For example, Salt Security reported that there was a 681% increase in API attacks in 2021, with a continued upward trend of attacks in the first quarter of 2022.

In addition to the risk of identity fraud and API attacks, there are also open issues related to data ownership, data use and transfer, and data storage and disposal. With consumer data being shared across financial institutions, fintechs, APIs and other platforms, the open banking rule and related regulations must address key questions, including:

- Who is responsible for protecting the data?
- What can be done with the data?
- How will the data be stored?
- What standards must APIs meet before data is exchanged between the financial institution and a third-party provider?
- What is the disposal process and timeline?
- Who is accountable in the event of a data breach that results in consumer data being compromised?
- Are consumers responsible for the risks associated with sharing their data?

These questions remain unanswered despite the push for the CFPB to issue the open banking rule.

So, how does the CFPB get the open banking rule across the finish line?

Perhaps U.S. regulators should consider how the European Union (EU) has successfully implemented open banking rules since 2009.

In the EU, open banking is heavily and uniformly regulated through the Payment Service Providers Directive 2 (PSD2), which requires banks to create APIs and open those APIs to third-party providers. PSD2 requires strong consumer authentication and directly regulates third-party providers through rules for data access and use. The uniform, stricter regulations that apply to the open banking market, including PSD2 and the General Data Protection Regulation (GDPR), increase data privacy protections and data security protocols and mitigate the potential of unauthorized access or improper use of consumer data.

Unlike the EU, the U.S. currently lacks uniform regulations or policies that can address open banking data privacy and security. The EU addressed uncertainty in open banking data privacy and security by standardizing the technology used to share data under PSD2, providing institutions with clear guidelines for data-sharing practices through the GDPR and enacting uniform regulations. A review of the EU's process may be instructive for the CFPB in addressing the U.S. open banking data privacy and security concerns.

Next Steps

The CFPB announced its regulatory agenda, which includes draft rulemaking under Section 1033, suggesting that the first rule for open banking could be ready before spring 2023.

The Small Business Regulatory Enforcement Fairness Act mandates that the CFPB seek feedback from a panel of small businesses about new regulations that may impact them. The next step in the CFPB's rulemaking process is for the proposed rule to undergo a small business panel review. Upon receipt, the small business panel has 60 days to review the rule and submit a report to the CFPB, at which time the agency can issue a draft final rule.

It is too early to determine how the open banking rule will address data privacy and security. Hopefully the CFPB will strike the right balance by implementing uniform regulations on open banking technology, privacy and cybersecurity for financial intuitions, fintechs and other third-party service providers.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Eyvonne Mallett . . . . . emallett@loeb.com

7049 REV1 09-09-2022