BANK POLICY INSTITUTE

A Short Prescription for Ensuring Responsible Open Banking in the United States

Stephanie Wake | September 9, 2021

The phrase "open banking" is used a lot these days, as policymakers push for consumers to have better control over their banking information, allowing them to access a wider range of products and services. The details of what exactly "open banking" means are generally not articulated, though the UK is often cited as a good model. Indeed, the UK took three important actions early on in its open banking effort that could serve as a model for the United States:

First, screen scraping was outlawed for accessing payment account data. Second, third-party providers (including FinTechs and data aggregators) were required to obtain regulatory permission and demonstrate appropriate data privacy, specialized insurance, and security measures in order to participate in open banking services. Third, participants were prohibited from gathering consumer data for any purpose other than providing the product or service for which the consumer provided authorization. The case for imposing these protections has only grown over time for the following reasons:

Data Aggregation through Screen Scraping Poses Serious Cybersecurity Risks – We shouldn't have to wait for a massive cyber breach of a data aggregator to recognize the cybersecurity concerns related to screen scraping for consumer financial data sharing, which enables aggregators to collect and store banking credentials (i.e., username and password). While screen scraping is nothing new – in fact, it extends back to the 1980s when it was developed primarily to minimize the need to re-enter data – its more recent use for granting third parties access to consumer bank accounts is problematic. Data aggregators have amassed hundreds of thousands, if not millions, of credentials, making them a prime target for a cyber-attack or data breach. Screen scraping also enables aggregators to gain access to data attributes beyond what is needed to provide the product or service requested by the consumer. For example, data aggregators do not need to obtain a consumer's demographic information or income details to sign that individual up for a Venmo account. A cyber-attack on a data aggregator would give a hacker unprecedented capability to drain or corrupt bank accounts.

Consumers Are Not Adequately Protected – Screen scraping has undoubtedly delivered a valuable service to many consumers by broadening the scope of digital offerings, but at what cost? After obtaining banking credentials, data aggregators can repeatedly scrape data from a consumers' bank account, and potentially share credentials or sell consumer information to other parties. With unfettered access to consumer account data through screen scraping, consumers sacrifice basic protections such as privacy and security and are at higher risk of fraudulent activity. Recent *lawsuits* against data aggregators, alleging that they used consumers' banking login credentials to scrape and sell consumers' financial data without their consent, underscore the consumer protection and privacy concerns related to screen scraping and data harvesting. Consumers should have full awareness and control over what information is shared, how it is shared and with whom it is shared. However, so long as data aggregators can continue to engage in screen scraping, consumers will have limited control over their data.

APIS – A SAFER ALTERNATIVE

The cybersecurity and consumer protection concerns associated with screen scraping are widely recognized across the financial sector. Restrictions of the type imposed by the UK would not meaningfully impede consumer access to data, as technology provides solutions. For these reasons, the banking industry in the United States continues to move away from screen scraping in favor of sharing consumer financial data through an Application Programming Interface (API) – the required standard in the UK. APIs are more accurate and more secure than screen scraping, as they allow data to be shared without the use of consumer credentials and provide enhanced control over the type and extent of data shared.

Several industry efforts have advanced the adoption of APIs in the United States. For example, the Financial Data Exchange developed a common API technical standard for data sharing through an industry consortium of banks, data aggregators, FinTechs and consumer groups. Over *22 million consumers* are now using FDX's API for data sharing in North America, in addition to the *3 million* in the UK. Additionally, banks and data aggregators have entered into data access agreements to facilitate the data sharing process through APIs and to specify how data is accessed and protected.

Notably, this transition to API-based data sharing in the United States has been driven by market forces, rather than a regulatory mandate, as occurred in the UK. In many ways, the market-driven approach has been appropriate for the United States given the fragmented structure of the banking industry, which consists of thousands of banks serving consumers and corporate customers, as compared to a few hundred in the UK, with nine large banks holding most of the market.

Despite the industry's progress, screen scraping remains a widely used method for accessing payments account data, enabling data harvesting of credentials to continue. In fact, some data aggregators want to reserve the right to screen-scrape data even after entering into data access agreements to utilize an API for data sharing. The question remains – why continue to allow aggregators to engage in these practices that put consumers at risk when more responsible and secure methods for consumer financial data sharing exist?

WHO'S RESPONSIBLE FOR OPEN BANKING IN THE UNITED STATES?

Unlike the UK, the United States does not have an open banking regulatory regime.[1] The analog most often referred to is the Consumer Financial Protection Bureau (CFPB), given its authority under section 1033 of the Dodd-Frank Act to promulgate rules around consumer financial data sharing. However, the CFPB cannot act alone; section 1033 requires the CFPB to consult with the federal banking agencies on its rulemaking efforts. With the increased sharing of consumer financial data to power new FinTech apps and products, regulators have essentially enabled sensitive financial data to leave a protected environment (the highly regulated banking industry) with no controls – this is a security concern in addition to a consumer protection concern, requiring coordination between the federal banking agencies and the CFPB.

The recent *Proposed Interagency Guidance on Third-Party Relationships*, which advises banks to conduct due diligence over data aggregators and monitor screen scraping activities, as well as the *FFIEC guidance on authentication*, referencing risk management for both credential and API-based authentication, emphasize the

[1] See "Payment Strategies Report: Modernizing U.S. Financial Services with Open Banking and APIs," Susan Pandy, Ph.D., Federal Reserve Bank of Boston (February 8, 2021), available at: Modernizing-US-Financial-Services-with-Open-Banking-and-APIs (1).pdf at 4 ("In 2015, the European Union mandated open banking and APIs under its Payment Services Directive 2 (PSD2) and General Data Protection Regulation (GDPR) to govern data protection and privacy for all EU residents. PSD2 requires FIs to provide TPPs access to customer data via open APIs. It also mandates that FIs and their TPPs implement related data security controls. These laws offer a framework for how FIs and TPPs can share data, and how TPPs should protect the consumer data they collect and use" (internal citations omitted)).

need for regulators to coordinate to ensure banks do not face dueling mandates between providing consumers access to their data and overseeing the practices of data aggregators.

THE ROAD AHEAD

As we move forward, here are three ways that U.S. regulators can strengthen the protections afforded to consumers as we continue to create an open banking regime:

First, the industry needs a specific timeline to outlaw screen scraping of payments account data and accelerate the migration to APIs. The technologies exist today, but market participants may not have the incentive to transition to APIs if screen scraping is allowed to continue. Regulatory involvement to outlaw screen scraping, either through an act of Congress or coordination between the CFPB and federal banking agencies in implementing section 1033, would further enable consumers to intentionally share their information in a safe and secure manner. Admittedly, requiring the thousands of banks, data aggregators and FinTechs in the United States to convert to APIs for sharing consumer data is no easy task, particularly for the smaller community banks that may not have the resources to develop and implement APIs. The transition will likely take years to fully implement. Continued support of FDX's efforts to develop industry standards, as well as efforts by Akoya to *integrate core providers* and data recipients into its API-based data access network, will help facilitate the transition. In addition to payments account data, the industry should consider outlawing screen scraping for wider range of financial products, as the UK is currently considering in its *transition to "open finance."*

Second, entities holding sensitive consumer financial data should be required to appropriately safeguard that data. Unlike the UK or European Union, the United States does not have in place national data privacy or security requirements. In the United States, banks are subject to data privacy and security standards under the Gramm-Leach-Bliley-Act (GLBA) and are regularly supervised by regulators. The CFPB, together with the Federal Trade Commission, should ensure that data aggregators, and other entities holding sensitive consumer financial data, are subject to the same standards as banks for safeguarding consumer data.

Third, the CFPB should limit the amount of data shared to only that which is necessary. To its credit, the CFPB requested comments on which data elements should apply to section 1033 within *its Advanced Notice of Proposed Rulemaking*. A "consumer financial data right" should not constitute unfettered access for third parties such as data aggregators. The end goal should be to create a data ecosystem that is highly protected and serves all consumers and market participants.

_____

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.