

Payment Strategies Report | February 8, 2021

Modernizing U.S. Financial Services with Open Banking and APIs

Susan Pandy, Ph.D., Federal Reserve Bank of Boston



Contents

Executive Summary	3
Introduction	3
U.S. Key Drivers of Open Banking and APIs	5
U.S. Financial Institution Perspectives.....	8
Conclusion	11

The views expressed in this paper are those of the author and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System.

Mention or display of a trademark, proprietary product or firm in this report does not constitute an endorsement or criticism by the Federal Reserve Bank of Boston or the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms.

The author would like to thank members of the MPIW and other industry stakeholders for their engagement and contributions to this report.

Executive Summary

It is important to understand the status of open banking¹ and application programming interfaces (APIs)² in the United States. Financial institutions (FIs) that have a vision for open banking may have an advantage over other FIs, as they re-evaluate existing operating models, invest in open technology architecture, and find new ways to work with ecosystem partners. Open banking is an essential path to innovation and FIs should be developing strategies to support this shift away from traditional banking models. Traditional models rely on FIs permitting data aggregators³ to use screen scraping technology⁴ to access to consumer login credentials for various accounts. The API is widely seen as a more secure and standardized method to make these connections on behalf of app users.

The objective of this whitepaper is to understand key developments, drivers, and considerations in the U.S. market that support progress towards open banking and APIs and how APIs offer a wide variety of new services. The U.S. has a multi-faceted approach to open banking characterized by both public and private developments. Third-party collaboration can lead to new product development. Opening a bank's platform to third-party applications can create synergies with innovative technology businesses to build a new generation of digital financial activities that enhance the consumer experience.

Introduction

A 2018 Celent study shows that approximately 20 U.S. FIs have open banking portals to facilitate third-party provider (TPP) access to consumer financial and other data.⁵ This number is expected to reach over 200 FIs by the end of 2021.^{6,7} According to Pew Charitable Trusts, between 2010 and 2018, U.S. investments in financial technology (FinTech) grew from almost \$2 billion to more than \$100 billion, with over half of the increase occurring in 2018 alone. Payments systems that move money between

¹ Open banking defines a system that offers businesses and customers a range of products and services based on open flows of data (often using application programming interfaces or APIs) as permitted by consumers. Open banking works with a broad range of financial services, including payments, giving consumers greater control over their financial data.

² An API allows the creation of applications that access the features or data of an operating system, application, or other service. APIs are a set of protocols and codes that determine how different software components can communicate (i.e., allows programs to talk to each other). The developer creates the API on the server and allows the client to talk to it.

³ Data aggregation is the compiling of information from databases with intent to prepare combined datasets for processing. Data aggregators are companies that collect information from other providers.

⁴ Screen scraping is the process of collecting screen display data from one application and translating it for another application to display.

⁵ Celent (2018, March 21). APIs in banking: Unlocking business value with banking as a platform (BAAP). Retrieved from <https://www.fidor.com/documents/analyst-reports/celent-apis-in-banking-unlocking-business-value-with-baap.PDF>.

⁶ Streeter, B (2020, July 27). Open banking gets a big jump start from Covid-19. *Financial Brand*. Retrieved from <https://thefinancialbrand.com/98831/open-banking-covid-fintech-tpg-digital/>.

⁷ Hines, K. (2020, July 11). The steady rise of open banking: Laying the foundations for open finance. *Celent*.

consumers and FIs will benefit from technology upgrades to their aging infrastructure.⁸ Ernst & Young reports that adoption of FinTech services has moved steadily upward, from 16 percent in 2015 to 64 percent in 2019. Awareness of FinTech is now very high, even among non-adopters, with 96 percent of global consumers aware of at least one alternative FinTech service that helps them transfer money and make payments.

Open banking is a global trend driven by innovation, regulation, the pace of FinTech, and consumer demand for more control over how their data is used. Open banking allows for the secure transmission of account data authorized by the customer to a TPP. FIs collaborate with TPPs and use APIs to enable new services and connect the FI application (app) to merchants, consumers, and companies. Significantly, open banking has moved the financial industry toward data modernization and decentralization. This represents a shift towards more open and cloud-based technology architectures, rethinking data management needs, and discovering new business partnerships. A key benefit of open banking is it allows FIs to offer customers enhanced financial services, greater control over their data, and data sharing with TPPs.

Over the last several years, U.S. FIs and TPPs have been monitoring open banking and API developments in Europe and other countries. The U.K. offers a useful test bed for open banking and important lessons to other countries planning to adopt it. In 2015, the European Union mandated open banking and APIs under its Payment Services Directive 2 (PSD2)⁹ and General Data Protection Regulation (GDPR)¹⁰ 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.¹¹ 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. As of the first quarter of 2020, there were approximately 300 TPPs registered under PSD2. Other countries, such as India and Australia, have followed the EU's approach.¹²

⁸ Pew Charitable Trusts (2020, Sept. 10). *Can regulators foster financial innovation and preserve consumer protections?* Retrieved from <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2020/09/can-regulators-foster-financial-innovation-and-preserve-consumer-protections>.

⁹ PSD2 is a data and technology-driven directive that aims to drive increased competition, innovation, and transparency across the European payments market, while also enhancing the security of internet payments and account access. A central requirement under PSD2 is for banks to grant TPPs access to a customer's online account/payment services in a secure, regulated environment.

¹⁰ The GDPR (EU) 2016/679 is a regulation on data protection and privacy for all individual citizens of the EU and European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The legislation was in substantial part intended to provide more robust protections for personal information and harmonize the regulatory environment for international business by unifying the regulation within the EU.

¹¹ PSD2 requires that FIs and TPPs conduct risk assessments and implement related controls to mitigate identified risks, monitor transactions to identify red flags, and report incidents to national authorities. It also requires FIs and TPPs to adopt "strong customer authentication (SCA)" methods to all but low-risk transactions. This includes the use of authentication codes that: 1) contain the relevant details of the transaction, and 2) are sent on a separate channel than the one that executes the transaction. It also requires customers to confirm at least two of three elements (i.e., multi-factor authentication) for all but the lowest-risk transactions.

¹² In May 2020, India released its Account Aggregator Framework, followed in July by Australia's mandate for open banking under its Consumer Data Rights Act.

U.S. Key Drivers of Open Banking and APIs

While regulation is driving open banking in other countries, U.S. regulators are letting the market drive this shift. However, some efforts by the Consumer Financial Protection Bureau (CFPB) and the U.S. Department of Treasury are noteworthy and recognized by the financial services industry as necessary to stimulate greater adoption. They are issuing non-binding guidelines that allow industry stakeholders to set the direction. In 2017, the CFPB published [*Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*](#).¹³ These principles focus on consumer control and transparency, informed consent, safety, security, data privacy, and accountability for ecosystem risks. Consumer control ensures that consumers can review where access to their data has been granted, who has that data, and how that access can be revoked. Some FIs view these principles as a strategic industry mandate, compared to PSD2's top-down approach. Accordingly, early adopters of these principles can develop their open banking strategies with some guidance, if they choose.

The CFPB plans to issue guidance in early 2021. The Bureau issued an [*Advance Notice of Proposed Rulemaking \(ANPR\)*](#) for consumer-authorized access to financial records with comments due by Feb. 4, 2021. Section 1033 of the Dodd-Frank Act deals with consumer access to financial records. Dodd-Frank 1033 states that: "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 received from such covered person ... in an electronic form usable by consumers" (12 U.S.C. §5533(a)).¹⁴ Consumers should be able to access their financial information to better monitor their finances and permit a third-party to access that information to provide innovation in financial services.

Third-party providers can use consumer digital financial records to offer value-added products and services to consumers. However, this expanded access to consumer financial data raises some serious concerns, noted in the CFPB ANPR and related to: data access and scope, credential-based access and screen scraping, disclosure and informed consent, privacy, transparency and control, security and data minimization, accuracy, disputes, and accountability and legal issues. FIs are concerned about sharing certain data such as personally identifiable information (PII) or account numbers, which create higher risk than other data. FIs also are unlikely to share what they consider proprietary information (e.g., account cost and pricing data, fees, account interest rates). However, aggregators believe this decision should be up to the consumer.

In 2018, the U.S. Treasury issued [*A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*](#), which compares open

¹³ U.S. Consumer Financial Protection Bureau. (2017, Oct. 18). *Consumer protection principles: Consumer-authorized financial data sharing and aggregation*. Retrieved from <https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/>.

¹⁴ See <https://uscode.house.gov/statutes/pl/111/203.pdf>.

Payment Strategies Report | Modernizing U.S. Financial Services with Open Banking and APIs

banking and faster payments.¹⁵ This document marked the beginning of modernization for the financial services industry. Both the CFPB and Treasury have created momentum that represents tangible progress for the ecosystem in its move towards more connected and open banking.

Several private sector initiatives are also driving U.S. adoption of open banking and APIs.

First, The Clearing House (TCH)¹⁶ created a [Model Data Access Agreement](#) that companies can leverage to develop their own data access and sharing agreements. TCH also acquired Akoya, a platform that serves as a single point of access for TPPs to access customer financial information.¹⁷ Akoya offers a centralized approach for broad integrations between FIs and TPPs, including messaging between parties. TPPs connect to Akoya using secure APIs to obtain access to the financial data of all the TCH FI participants. However, FIs must integrate with Akoya to support these APIs, which can take several months to one year. This requires FIs to manage infrastructure products, customer messaging, and API performance.

Second, several industry groups have created frameworks to develop common standards for open banking. The Financial Data Exchange (FDX) has aligned a cross-section of FIs, FinTechs, large technology companies, and card networks around a common data-sharing standard, the Representational State Transfer (RESTful)-based API, to accelerate the adoption of open banking API frameworks and standardize the transfer of data.¹⁸ In previous years, Simple Object Access Protocol (SOAP)-based APIs based on XML were used.¹⁹ REST uses a more modern language, known as JSON.²⁰ REST is a set of rules that developers follow to create their APIs. FDX also issued industry recommendations for obtaining user consent to share information and monitoring API performance.

¹⁵ U.S. Department of Treasury. (2018, July). *A financial system that creates economic opportunities - Nonbank financials, fintech, and innovation*. Retrieved from https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

¹⁶ Established in 1853, TCH is the oldest banking association and payments company in the U.S. and is owned by 24 of largest U.S. leading commercial banks, for which it provides payment, clearing, and settlement services.

¹⁷ See <https://www.akoya.com/>.

¹⁸ Financial Data Exchange (FDX) was created in 2018 as a standards-setting group and has more than 150 members, including financial institutions, large technology companies, card networks, and FinTechs. See <https://financialdataexchange.org/>.

¹⁹ Simple Object Access Protocol is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP), although some legacy systems communicate over Simple Mail Transfer Protocol (SMTP) for message negotiation and transmission.

²⁰ JSON is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and array data types. It is a very common data format with a diverse range of applications.

Payment Strategies Report | Modernizing U.S. Financial Services with Open Banking and APIs

The National Automated Clearing House Association (NACHA)²¹ partnered with Accenture to create the API Standardization Industry Group (ASIG) to develop a tool for FIs, businesses, FinTechs, and other industry stakeholders to standardize the use of APIs. ASIG has identified 16 APIs across three categories for further development based on their overall impact to the payments industry: 1) fraud and risk reduction, 2) data sharing, and 3) payment access.²²

The Financial Services Information Sharing and Analysis Center (FS-ISAC) has also developed an API to support the secure transfer of data that aligns with PSD2 requirements to help FIs use uniform systems when conducting business in the U.S. and EU.²³

Third, Mastercard acquired Fincity making it a gatekeeper for FinTech and open banking activities. Visa attempted to acquire Plaid in 2020, but this acquisition was stopped by the U.S. Department of Justice in early 2021. Plaid delivers an API platform for TPPs to connect to FIs for account access and authentication. Fincity provides access to financial data in real time. Data aggregators serve as central hubs for sharing bank account data with all the applications that need it. These aggregators collect data and feed it into FinTech apps, such as Acorns, Betterment, Chime, Transferwise, and Venmo. Many stakeholders view such acquisitions as an indication that open banking is the future of consumer and small business financial services and that these services can benefit FIs as the biggest customers of the card networks.

Financial institutions and technology companies are providing the impetus for open banking in the U.S. through enhanced and expanded digital services to their customers. Some FIs look to the large technology companies that have succeeded in their use of APIs, such as Expedia, Facebook, Google, Intuit, and Stripe. For example, in 2017, Wells Fargo entered a data exchange agreement with Intuit to expand functionality by giving their shared customers greater control over their financial data.²⁴ Technology companies, such as Envestnet Yodlee, offer financial data APIs that provide access to the majority of U.S. FIs. Stripe connects its API systems to FI platforms. Expedia provides API-based tools and technology to over 10,000 partners in 33 countries to turn its web traffic into hotel bookings and satisfied customers.

FIs have been following API developments for several years. While TCH provides a model agreement, many large FIs have created their own data-sharing agreements, often based on some of the CFPB principles, such as security, customer control, transparency, and privacy. Some FIs have looked at FDX for guidance to help FIs create a set of principles for developing customer-permissioned data sharing. FIs need to understand

²¹ NACHA is a nonprofit organization that convenes hundreds of diverse organizations to enhance and enable ACH payments and financial data exchange within the U.S. and across geographies. See www.nacha.org.

²² For more information, see <https://www.nacha.org/content/api-standardization>.

²³ Morgan, Rob. (2018, Feb. 13). FS-ISAC announces API to facilitate customer data sharing. *ABA Banking Journal*. Retrieved from <https://bankingjournal.aba.com/2018/02/fs-isac-announces-api-to-facilitate-customer-data-sharing/>.

²⁴ Palmer, Greg (2019, Jan. 4). It's safe to bet on open banking. *Fintech Futures*. Retrieved from <https://www.fintechfutures.com/2019/01/its-safe-to-bet-on-open-banking/>.

what data is shared, the duration period for sharing that data, and how the customer can revoke the data-sharing arrangement. FIs also want to ensure that the customer understands how the TPP will use the data. For data privacy, the FIs require that only the minimum level of data is shared and not used for purposes other than those intended by the TPP app. The FI agreements also outline the obligations of the TPP to protect customer data and comply with the FI's cybersecurity standards. Data-sharing agreements between FIs and TPPs are a critical piece of the open banking puzzle as the parties define expectations, make agreements, and identify consumer expectations.

U.S. FIs view open banking as a catalyst for digital transformation and recognize that data management is now as important as money management. However, they face challenges related to reliance on legacy systems and the complexities of automation and digitalization. While many large FIs are moving to cloud-based infrastructure, the cost of scalability impedes implementation. FIs may have to consider new business models to accelerate digitization and remain competitive.

U.S. Financial Institution Perspectives

There are many ways that FIs can leverage open banking and APIs internally or externally using TPPs for commercial business, retail (consumer), customer consent, payment request authorization, and authentication.²⁵ This whitepaper primarily discusses the retail aspects based on interviews with several large FIs and other companies. U.S. FIs consider open banking as a way to obtain customer-permissioned access to financial data. Some FIs want to understand how to leverage data to generate new value for customers and new revenue streams to monetize the value of their APIs when they grant access to TPPs. FIs that use APIs for commercial business seek to address corporate banking challenges as well as opportunities for small business customers. FIs with retail business are using account aggregation to allow consumers to see their entire financial account positions. The retail approach may not be as profitable as commercial applications for open banking, but it helps FIs deepen the customer relationship and remain competitive.

An Oracle 2018 global retail banking survey showed that consumers are demanding smarter and more relevant digital banking experiences. Approximately 69 percent of consumers want their entire financial lifecycle on digital channels and 30 percent are open to trying a FinTech or challenger bank.²⁶ In response, FIs are offering new alternatives to increase consumer engagement. U.S. consumer preferences for open banking are mixed. A 2019 Deloitte survey showed that consumers seem receptive to the concept. One in five U.S. consumers finding open banking valuable, with more interest among millennials (born between 1981-1996, 39 percent) and Gen X consumers (born

²⁵ The API is considered a gateway within an FI, in that everyone authenticates through the API, both internally and externally.

²⁶ Oracle Financial Services. (2018). *The new digital demand in retail banking: From customer experience to engagement across life moments*. Oracle Financial Services Global Retail Banking Survey 2018. Retrieved from <https://www.oracle.com/a/ocom/docs/dc/new-digital-demand.pdf>.

between 1965-1980, 50 percent).²⁷ Despite privacy and security concerns in the use of their personal information, consumers expressed interest in easier financial services and management, including the ability to compare bank services, integrate financial data, and personalize budgeting tools.

Customer-focused models

A common thread across the interviews is the focus on the customer. Within the last five years, large FIs have realized that they can no longer keep customers within their strictly controlled systems of collected data. FIs need to shift from a system designed to keep data tightly controlled to an open architecture where customers can share data with their chosen TPPs. Allowing users to co-manage their data is becoming a requirement of customer retention.

Prior to open banking, some FIs shared customer usernames and passwords with TPPs and aggregators through screen scraping, but the industry is moving away from this model. Some FIs still rely on screen scraping but do so through APIs. Ultimately, the impetus is to ensure customers can safely and securely share their data with a TPP app without sharing their bank login credentials. This provides customers with more control over how their data is accessed and used. In the past, TPP apps screen scraped an FI's website to perform account owner verification or obtain the deposit account number. Once an FI enables a TPP to verify the customer's account and routing number, the TPP app (e.g., Acorns, Robinhood) can authorize a payment using a preferred funding method (e.g., ACH, debit, credit, prepaid) and eliminate manual entry of the data to reduce friction. APIs can achieve this functionality and provide the account data safely and securely.

This model remains a considerable security risk to the payment ecosystem, as more data than is necessary is stored or shared, especially if the TPP app or aggregator stores the customer's account number. This underscores the lack of consumer understanding about with whom they share their credentials or account information. According to 2019 TCH research, 80 percent of consumers were unaware that they were not logging into their FI website, but rather sharing their login credentials with a TPP to provide access to their bank account data. This highlights the contradictory advice given by many FIs, which warns consumers not to share their login credentials to avoid fraud and phishing attacks, while simultaneously allowing consumers to share their login credentials with TPPs to access alternative financial services.

To build the API foundation, the FI must obtain the customer's consent for data sharing and allow the customer to select the data they want to share. Consent and data selection occur through an API, using the OAUTH v.2.0 protocol.²⁸ The API can also

²⁷ Deloitte (2019, Oct.). *Open banking: switch or stick? Insights into customer switching behavior and trust*. Retrieved from http://images.content.deloitte.com.au/Web/DELOITTEAUSTRALIA/%7Bc4424870-fdef-4b12-b03a-d7203fa9b14a%7D_OpenBanking_Survey_2019_final.pdf?elq_mid=2642&elq_cid=280819.

²⁸ OAUTH v.2.0 is an open standard authorization protocol that provides customers with access to their data on websites and in social media apps without the need to use login credentials. It is the standard for secure access to APIs and fosters ease of access for the end user.

support account verification functionality. Financial institutions can use APIs to share different types of information, including general account data, balance data with PII for personal financial management (PFM) transactions, tax documentation, or customer profile data (e.g., name and email address). Some APIs support use cases for money movement using the customer's actual or tokenized account credentials.

The FI allows the customer to select data at the account level and notifies them about the types of data that will be shared with the TPP (e.g., Venmo). The Venmo app does not have access to the customer's bank account balance, interest rate, or username and password. The customer clicks on the "I authorize" option with an aggregator or TPP, which permits them to call the FI's API for that specific use case (e.g., Venmo person-to-person payment, PFM transaction). The customer authorization occurs within the FI's online or mobile banking platform during the TPP money movement process. The customer can see that they authorized Venmo to withdraw and send funds based on certain data, but they cannot withdraw that authorization or consent to access the data.

Many FIs also leverage OAUTH to create an access token in lieu of the customer's login credentials to share with TPPs and aggregators. The technology has two components: 1) the token to grant access to the account based on OAUTH, and 2) the API that allows the transfer of customer data from the FI to the TPP. On the back end, the FI has an agreement with the TPP to verify various customer data factors, such as the internet protocol (IP) address or knowledge-based authentication factors, before sharing the access token with the TPP.

FIs may offer customers a dashboard with added visibility into how and where their data is being shared. For example, Chase offers "Account Face" through its mobile banking app. The dashboard enables the customer to revoke access to their data at any time to minimize data exchange and prevent data misuse.

Beyond consumer benefits, many FIs think about open APIs in terms of building industry collaboration and partnerships by expanding their use across the FI enterprise and into commercial business operations. Partnerships allow for data sharing and the ability for customers to open new bank accounts.

Enterprise or commercial payments

Commercial FI clients move money and seek various tools to facilitate transactions and collect transaction and invoice data. APIs between FIs and corporate customers allow for secure information sharing. For example, one large FI uses a closed-loop API for its vehicle fleet management program. The FI provides data about the fleet driver and the merchant for the fleet payment cards. Telematics²⁹ can track fleet drivers to ensure that

²⁹ Telematics is an interdisciplinary field that encompasses telecommunications, vehicular technologies (road transport, road safety), electrical engineering (sensors, instrumentation, wireless communications), and computer science (multimedia, Internet). Telematics can involve: 1) technology of sending, receiving and storing information using telecommunication devices to control remote objects; 2) integrated use of telecommunications and informatics for application in vehicles and to control vehicles in transit; 3) global navigation satellite system technology integrated with computers and mobile technology in automotive navigation systems; and 4) use of such systems within road vehicles.

they follow the prescribed route, drive efficiently, and conduct fuel tests. The API for the fleet program addresses issues such as fuel fraud. Since the data itself is unchanged, use of APIs is low-risk.

Some FIs have also created developer portals for TPPs and FinTechs which are still evolving. The portals follow a self-serve model with the necessary security controls. Companies that register to use an API must comply with FI security, risk, and privacy requirements. Citi was the first U.S. bank to create a developer portal for APIs.

Partnerships and collaboration

FDX is facilitating much of the collaboration noted above through member participation. FDX has been particularly helpful in supporting industry inclusiveness. Many smaller FIs or FinTechs may not have the resources to pursue partnerships, but FDX participation reduces the burden to acquire market knowledge and deliver value to the industry. Some FIs are also working with TCH to develop and align best practices around security, customer value, and market efficiencies. There is an overall desire by groups like FDX and TCH to help the industry align around a ubiquitous standard that helps to ensure the system is safe and secure while working toward optimal efficiency.

Conclusion

Open banking represents a significant industry trend that catalyzes innovation and efficiency across the payments ecosystem and other verticals. The COVID-19 global pandemic may accelerate this momentum towards a full open banking infrastructure in the U.S., given the demand for expanded connectivity in an environment that is becoming less dependent on an in-person model. The pandemic has also spurred interest and demand for PFM budgeting, savings, and financial management tools.

Most FIs will have to support open banking and APIs for their retail businesses in order to stay competitive. Successful models will customize the consumer or corporate client experience. For retail banking, the impetus is less about revenue generation than it is about sustaining customer loyalty and retention. The end state for FIs is to remain at the center of the customer's permissioned data, which makes the relationship stickier. However, it is too soon to know if customers will find this valuable and trust that their data will remain private and secure.

Consumer preferences and level of comprehension are still unclear. Important questions remain about how to properly treat consumer data and the measures needed to ensure that consumers are protected. U.S. FIs, FinTech, and TPPs need to provide security and education about open banking and related services prior to a formal rollout. Open banking can create a paradigm shift in how FIs treat the issue of ownership, storage, and use of data.

However, several risks and challenges need to be addressed. The industry is waiting for guidance from the CFPB. Interoperability is lacking and many FIs struggle to replace legacy infrastructures with fully digital platforms, which can require considerable

Payment Strategies Report | Modernizing U.S. Financial Services with Open Banking and APIs

investment. FIs may be struggling to prioritize open banking and API permissioned data with competing projects.

The largest U.S. FIs have been investing in APIs for several years, so the biggest opportunity should be for the large FIs to extend open banking benefits to smaller and mid-sized FIs through their core processors.

Other considerations include how faster payment initiatives may interact with open banking and APIs. FinTechs are looking at real-time payments (RTP) services, as they will need access to consumer financial data (e.g., account number) via APIs to provide their services. As a potential new faster payment use case, open banking should be closely monitored for API fraud.

There is consensus across the payments industry that an open banking model is necessary. However, not all stakeholders agree on how this should be accomplished. Some are concerned about the impact to current business models and additional requirements needed for a new business model. Another concern is whether there will be a level playing field for FIs and FinTechs. For example, open APIs enable seamless data flows between FIs and TPPs, which in turn have the potential to greatly enhance services for customers. APIs also allow FIs to share data with strategic partners and accelerate innovation, but this is contingent on standardization of data-sharing technologies.

In the future, many open banking and payment services will likely be conducted via mobile phone. Mobile wallets are cost-effective, ubiquitous, and positioned to adapt to evolving consumer needs for personalized financial services. Mobile wallets can also strengthen security as an authentication tool.

If the U.S. is moving towards advancing open banking, it may be helpful for U.S. regulatory agencies, such as the Federal Reserve Board of Governors, Federal Trade Commission, and CFPB, to conduct a study on consumer preferences and perceptions of open banking while the U.S. market is still in its infancy.