American Bankers Association®

Understanding APIs

Technology has facilitated the creation of unprecedented amounts of consumer financial data, providing new opportunities to deliver innovative banking experiences. As the amount of data has grown, so too have the number of third parties interested in leveraging it to offer additional financial services. In many cases, consumers must permit access to certain financial account data in order to use these services.

To date, this data access has been facilitated via a process known as screen scraping. Banks have serious concerns with screen scraping, as it requires customers to forfeit their login credentials and may expose them to risks that the customers do not fully understand. Banks are working to facilitate secure data transmission between banks and authorized third parties.

APIs, short for Application Program Interfaces, are promising tools to address this challenge. APIs allow for the secure transmission of data between systems in a standardized format. This can empower customers to share financial data without forfeiting their sensitive user credentials while allowing banks to provide customers with the security, control, and transparency they deserve.

What Are APIs?

Any bank that has integrated a third-party service or completed an acquisition understands the effort required to get different systems to communicate with each other. APIs are tools that do just that. Acting as a sort of universal adaptor for data, APIs create a common language for different systems to communicate and exchange information.

APIs are what allow Facebook users to sign into third-party services with their Facebook accounts. When a user opts to sign into Spotify via Facebook, for instance, the connection is made through an API that enables Spotify to verify the user's identity and upload any necessary user information.

Traditionally, APIs have been proprietary, non-standardized, and designed for internal use only.[1] Today, the industry is developing open API standards that can facilitate data-sharing between companies.

Open APIs are accessible to developers outside an organization. While third parties may need to meet certain standards to qualify for access, no additional infrastructure is required to connect into them.[2] Developers can code to the APIs specific criteria, enabling access to linked systems.

So, how do APIs enable data transmission? There are two key components. First, one must authenticate the identity of the party accessing the API and verify that they have been granted account access by the user. Second, one needs to transmit the data from point A to point B.

[1] "Open APIs: A Survival Guide for Banks." Finastra, 2017.

[2] Ibid.

Authentication

The first step in the exchange of financial data is authentication—the process by which a user, who has verified their identity, gives permission to an application to access data that resides elsewhere.

Historically, authentication was accomplished with login credentials. Users would verify their identity by sharing their username and password with an application. The application would retain those credentials and forward them to the API to access relevant data.[3] This process exposes banks and customers to security threats. The first rule of data security is not to share your password with strangers. When login credentials are shared banks have no way to distinguish legitimate customer logins from those of screen scraping applications or differentiate good actors from malicious ones.

To address these problems, Open Authentication (OAuth) was introduced in 2007. OAuth uses tokenization to verify data requests. Tokenization is the process by which sensitive customer information, like an account password, is substituted with a non-sensitive token that reduces the ability of bad actors to do harm. OAuth prevents an application from accessing a customer's credentials by relaying the customer from the third party's page to a login page on the APIs native server.[4] The API then returns an access token for that user to the application.

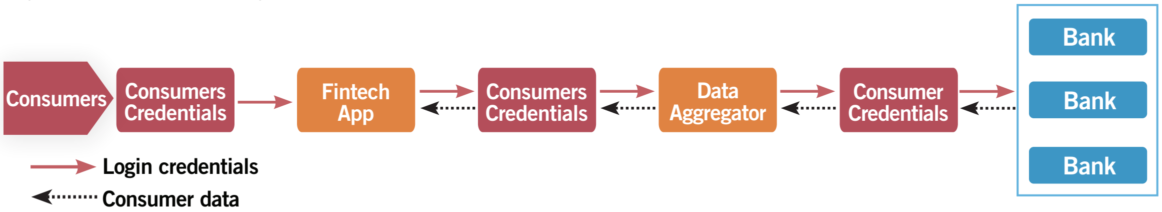
OAuth provides banks and their customers more control over how data is accessed and used.[5] When a user logs into an application for the first time via Facebook, for example, a window explains which user permissions are required (location, friends list, etc.). Access tokens may be used to restrict permissions to specific data sets. They can also be deleted in the event of a security breach, a user request, or misuse by the application—which effectively terminates third-party permissions.[6]

Data Transmission

The second step is transmitting the data from one party to another. Currently, many applications leverage a technique known as screen scraping to move customer data. Screen scraping refers to the process by which an application logs in to an account on behalf of a customer and uses algorithms to read or "scrape" the data presented on the screen as the customer would see it.

When users share their login credentials and authorize screen scraping, they give the application carte blanche access to their financial data. This can expose customers to risk, as they are giving a third-party full access to their account—even potentially the ability to execute transactions rather than sharing the specific information needed to power the third-party application.

Figure 1: Screen Scraping



Source: Treasury Fintech Report

[3] Stowe, Michael. 2015. Undisturbed REST: A Guide to Designing the Perfect API. Ebook. San Francisco: MuleSoft.

[4] Ibid., 60

[5] Ibid.

[6] Ibid.

Open financial exchange (OFX) is a more secure data transmission alternative that has been adopted by more than 7,000 financial institutions. OFX was developed in 1997 to ease the transfer of financial data among institutions. However, OFX does not support the exchange of several new types of financial data (such as extensive identity information or complex account types) and relies on an older, less flexible architecture and data formats.

In an effort to improve data exchange relative to OFX, a working group from the Financial Services - Information Sharing and Analysis Center (FS-ISAC) developed the Durable Data API (DDA) in 2015. DDA is a more flexible data transmission specification that allows for modern data formats. FS-ISAC has since launched the Financial Data Exchange (FDX) organization to facilitate the secure sharing of customers' data. More information about FDX can be found below in the Market and Regulatory Developments section.

Leveraging APIs

While APIs can reduce risks associated with screen scraping, they can also provide new opportunities for banks. Banks have used proprietary, non-standardized APIs for years to connect disparate back-end systems and to integrate third-party vendor services. Vendors need to customize for each bank partner or even each individual system within a bank. Standardized, open APIs can streamline the integration of third-party vendor services at lower costs for banks of all sizes and enable a concept called "open banking."

Third-party Vendor Integration

Community banks rely heavily on their core providers for their technology needs. Often, the cores charge hefty integration fees to banks looking to partner with third-party vendors. Moreover, due to the outdated WSDL file description format many cores use, vendors may be uncertain what data they will be able to access or what format it will be delivered in following integration—complicating implementation. The ability to bring new products to market quickly is critical for banks' ability to stay competitive with their peers.

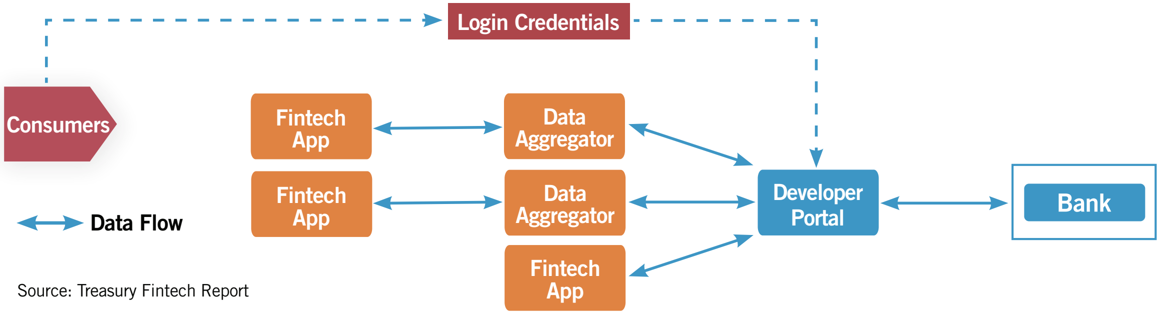
Industry efforts (e.g., FDX) exist to standardize various elements of APIs—like how data is stored, organized, and accessed—to streamline the integration process. The technical work required to launch these tools is largely out of community banks' hands. Community banks that receive technology services and support from a core processor should ask their core what steps they are taking to facilitate safe and secure data transmission. Once open APIs are deployed, community banks will need to understand what data the vendor will require and authorize that access.

Open Banking

Open APIs will enable "open banking," where every bank customer can easily access his or her financial data and permission access to third parties in order to use their services. Banks are actively developing ways to facilitate secure data transmission to enable this access.

Some banks have developed their own suite of API solutions to allow permissioned data access to developers. These developer portals give banks control over the architecture and design of the API and the processes and requirements necessary to access customer data. Authorized developers can then use the APIs to build new products and services. Developer portals enable banks to provide their customers with secure access to a broader array of digital products and services, and enable tech-savvy business clients to develop their own bespoke banking services.

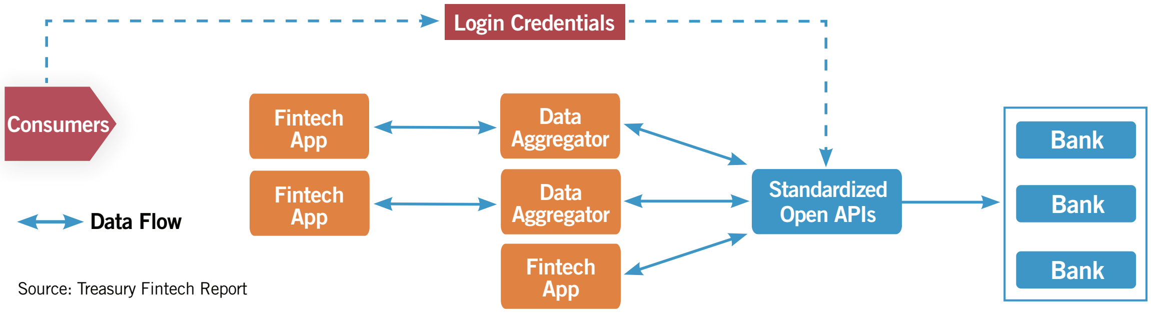
Figure 2: API Developer Portal



Source: Treasury Fintech Report

Today, APIs vary from institution to institution. Banks employ different nomenclatures for common terms and processes.[7] Industry efforts exist to drive standardized open APIs that would reduce the customization required by developers. More information about these efforts can be found below in the Market and Regulatory Developments section.

Figure 3: Standardized Open APIs



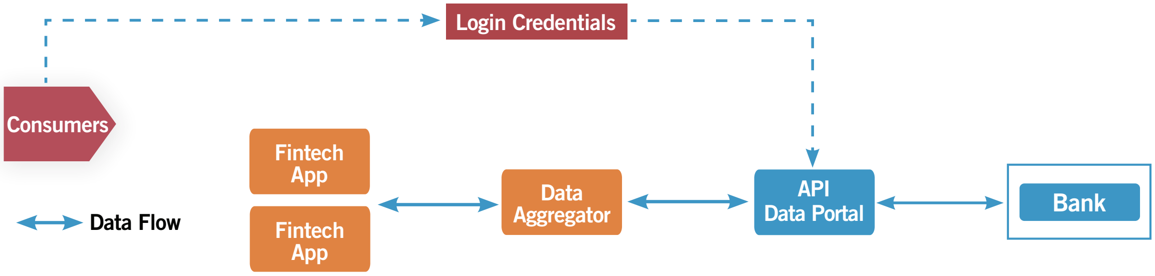
Source: Treasury Fintech Report

Other banks have formed partnerships with data aggregators and third-party service providers to facilitate secure data transmission through API data portals. Data aggregators collect and organize consumer financial data from various sources and then provide access to that data to fintech developers via their own APIs. According to Federal Reserve Governor Lael Brainard, banks that partner with aggregators can open their system to developers without having to invest in creating and maintaining their own suite of APIs.[8]

[7] "API Standardization – Shaping the Financial Services Industry." NACHA, 15 August 2018.

[8] Brainard, Lael. "Where Do Banks Fit In The Fintech Stack?" Board of Governors of the Federal Reserve System. Speech, Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research and Practice." 28 April 2017.

Figure 4: API Data Portal



Source: Treasury Fintech Report

Due to resource constraints, community banks may be unable to build APIs in-house or negotiate and oversee data-sharing agreements with aggregators. Technology firms exist that can provide API-as-a-service support for banks that require technological expertise related to developing API data and developer portals. Alternatively, banks can strike individual partnerships with fintech firms that are capable of integrating their services into a bank's system.

As mentioned above, community banks that receive technology services and support from a core processor may require the coordination of their provider to enable open banking capabilities. Banks should discuss what options are available for facilitating safe and secure data transmission with their core processors.

Open Banking Business Models

Open banking will provide new opportunities and enable new business models in the financial services industry. The models chosen by banks will likely vary depending on the unique strengths of each institution.

Utility:

Banks may choose to focus primarily on developing products and services and providing infrastructure for third-party financial service firms. For example, a bank based in Delaware provided the infrastructure necessary to hold deposits for the customers of Simple, a digital-only bank. This strategy may be valuable to banks that wish to offer compliance-as-a-service to new financial service entrants attempting to navigate the complex regulatory landscape. However, these banks will likely have fewer consumer interactions and, therefore, may have trouble developing strong customer relationships.

Aggregator:

Alternatively, banks may choose to focus on providing external developers with access to open APIs that enable them to offer their services from within the bank's platform. These banks will source products and services from a host of partners to provide customers with a broad array of financial solutions while saving costs related to internal product development. This will enable these banks to better satisfy customer's varied product needs. However, these banks may face some difficulty differentiating themselves from others in the market.

Platform:

The platform model builds on top of the aggregator model by recognizing and focusing on the unique strengths of a bank. These banks will leverage open APIs to integrate various third-party solutions alongside their own services to foster strong customer relationships. Bank app stores with vetted third-party products (similar to the Apple App Store) will enable customers to build their own personalized banking experience within the brand they trust. The platform strategy will enable banks to better differentiate themselves from others in the market. However, this model may be difficult to successfully implement without sufficient economies of scale and developer buy-in.

Market and Regulatory Developments

The industry has taken many steps towards API standardization and implementation. Regulators have also begun to explore the implications APIs present to the financial services industry.

Bureau of Consumer Financial Protection

The Dodd-Frank Act provides consumer rights to access financial account data in a usable electronic form. In November 2016, the bureau issued a request for information regarding consumers' ability to permission third-party access to account information. In a comment letter, ABA advised the bureau ensure consumer account data is subject to Gramm-Leach-Bliley Act (GLBA) protections regardless of where it is held; require third parties provide clear disclosures of how data will be used; and empower consumers to control how their data is shared.

In October 2017, the Bureau issued nine guiding principles for protecting consumers that share their financial data. The principles establish that third parties that are granted access to customer data should use it only to the extent necessary to provide the products and services selected by the customer, and that the data should be accessed, stored and used safely and securely. The bureau noted that consumers should not be required to give up their banking credentials. In addition, the bureau emphasized that consumers should have the ability to quickly review who has access to their data and have disputes over unauthorized access resolved in a timely manner.

Treasury Fintech Report

In July 2018, the Treasury Department published an extensive report recommending changes to laws and regulations affecting nonbank financial providers and the broader fintech environment. The report included a number of recommendations related to data access.

Treasury sees a need to remove legal and regulatory barriers to data sharing agreements that move firms away from screen scraping. Any solution, Treasury wrote, should be developed by the private sector, address resolution of liability for data access, address standardization of data elements, and explore efforts to mitigate implementation costs for community banks. Treasury recommended that the Bureau work with the private sector to develop plain language consumer disclosures and terms and conditions for how data is shared and used, and that consumers should be able to revoke prior authorization. Finally, Treasury recommended that banking regulators clarify how third-party guidance impacts data sharing agreements.

Financial Data Exchange

In October 2018, financial institutions, fintech firms, and industry groups announced the launch of the Financial Data Exchange (FDX), a non-profit organization to unify the financial sector around the secure exchange of financial data. FDX, a subsidiary of FS-ISAC, plans to address common challenges around the way the industry shares consumer account information to enhance security, innovation, and consumer controls.

FDX has introduced an interoperable standard and operating framework based on the DDA that gives consumers more choices about safely granting or revoking permissions to their banking data. The DDA will replace the need for screen scraping and credential sharing. When permissioned by consumers, financial institutions will have a consistent process for securely sharing consumer data with third parties.

FDX's board of directors comprises: Bank of America, BB&T, Capital One, Charles Schwab, Citigroup, Experian, Fannie Mae, Fidelity Investments, Finicity, FS-ISAC, Intuit, JPMorgan Chase, PNC Bank, N.A., Quicken Loans, SIFMA, TD Bank, TCH, USAA, U.S. Bank, Wells Fargo, Xero, and Yodlee.

NACHA

In the spring of 2017, NACHA formally created the API Standardization Industry Group (ASIG). ASIG was established to support the advancement and use of standardized APIs within the U.S. financial services industry. Membership includes more than 100 organizations representing diversified stakeholders. The group has published a white paper and has identified at least 16 API use cases related to fraud and risk reduction, data sharing, and payment access.

In September 2018, NACHA announced the launch of Afinis—a membership-based standards organization to develop "implementable, interoperable, and portable standards across operating environments and platforms."

Federal Reserve Board Governor Lael Brainard

In April 2017, former Federal Reserve Board Governor Lael Brainard discussed the implications of open banking. Some of the key underpinnings of consumer protection in financial services, Brainard said, sit uneasily alongside the openness, connectivity, and data access that enable today's app ecosystem. Brainard believes there may be need to re-examine vendor risk management guidance in the context of open banking. Safety and soundness regulations is shared among the banking regulators. Efforts to enable secure data transmission will require the engagement of multiple agencies, along with input from the private sector and other stakeholders.

Brainard discussed the consumer perspective of open banking in November 2017. "Consumers need to know and decide who they are contracting with, what data of theirs is being used by whom and for what purpose, how to revoke data access and delete stored data, and how to seek relief if things go wrong," Brainard said. "In addition, consumers should receive clear disclosure of the factors that are reflected in the recommendations they receive."

PSD2 in Europe

European Union member states this year were required to start implementing the revised Payment Services Directive (PSD2). Among other requirements, PSD2 created licensing regimes for third parties that access bank accounts for purposes of initiating payment orders or consolidating information with consumers' consent. The directive mandates that banks allow consumer-authorized third parties to access their consumer accounts without premising such access on contractual agreements with the banks. Credit institutions are required to provide detailed reasoning if they reject such access.

Conclusion

Banks can benefit greatly by effectively integrating APIs into their IT infrastructure. APIs allow banks to transmit customer information to authorized third parties in a secure manner, which reduces risks related to screen scraping for both banks and customers. This enables banks to empower customers to use a variety of ancillary financial services that can improve consumer financial wellbeing.

Moreover, once deployed, APIs enable banks to quickly and securely integrate third-party services into their systems to offer customers the latest technologies. Instead of dedicating resources towards expensive system integrations for each third-party firm, banks can allow vetted third parties to plug into their APIs in order to access the requisite data for the service to function. Banks that work on implementing APIs today stand to benefit the most in the open banking ecosystem of the future.