Beyond Compliance: Using Banking API Standards for Competitive Advantage

Published 3 December 2020 - ID G00733322 - 16 min read

By Analysts Mark O’Neill, Andrew Steadman, Don Free

Initiatives: Application Architecture, Development, Integration and Platforms; Application and Product Portfolio Governance; Financial Services Technology Modernization and Transformation

Open banking regulations are spreading worldwide, but creating APIs only for compliance can lead to poor API uptake and developer dissatisfaction. Application leaders should create differentiating API products that go beyond regulatory compliance, including leveraging standards such as BIAN and FDX.

Overview

Key Challenges

- Application leaders who have built APIs simply to comply with open banking regulations have not experienced the expected benefits to their bank, to fintech partners or to customers.

- “Screen-scraping,” whereby fintech aggregators access banking data on behalf of customers using the customer's own banking credentials, remains widespread. Application leaders who adopt a strategy to block aggregators risk alienating their own customers.

- API standards driven by open banking regulations focus on retail banking use cases, leaving application leaders in corporate banking without a similar set of API standards.

Recommendations

As an application leader responsible for application architecture, you should:

- Create differentiating API products which go beyond open banking compliance and are suitable for direct or indirect monetization in an API marketplace model.

- Incorporate API standards such as financial data exchange (FDX) to provide an alternative to screen-scraping, but ensure these do not introduce undue complexity to the customer.

- Add APIs for real-time corporate banking integration, to augment existing batch file-based connections to institutional clients.

Introduction
Open banking regulations, such as PSD2 in EU countries, require banks to provide APIs. Figure 1 shows banking API regulatory approaches worldwide, while Note 1 provides details of each country highlighted.

**Figure 1: Open Banking Regulations Worldwide**

However, simply implementing banking API regulations carries the risk of undifferentiation and poor API uptake. In countries without open banking regulations, Gartner speaks to API consumers who struggle with inconsistent, or often nonexistent, banking APIs. The consequence is that fintech API aggregators have stepped in with well-designed APIs which connect to multiple banks, even to banks without APIs (often achieved through “screen-scraping”), thus disintermediating banks. How can application leaders at banks deliver a successful API strategy? The answer is to go beyond mandated open banking standards and deliver differentiating API products.

In this research note we examine the state of banking APIs in open banking, banking aggregation and corporate banking. We provide recommendations for a successful banking API strategy, using examples including ABN AMRO, Standard Chartered Bank, Lloyds Banking Group and Citizens Bank.

**Analysis**
Create Differentiating API Products Which Go Beyond Open Banking Compliance

The State of Open Banking APIs

As shown in Figure 1 above, the focus of banking API regulations differs worldwide. Some countries take a “top-down” approach, such as the U.K.’s Open Banking which mandates that banks provide APIs for access to accounts (A2A) and payments using defined API standards, or India, where government regulations focus on APIs for payments (Unified Payments Interface [UPI]). Other countries, notably the U.S. and China, adopt a more “bottom-up” market-driven approach. Some countries combine the two approaches — mixing an organic market-driven approach with light governance. An example of this combined approach is how the Monetary Authority of Singapore (MAS) has allowed banks to define their own “API playbook” supporting common use cases, but keeps an API registry of banks which provide APIs.

In countries with a “top-down” regulatory-driven approach, banks have struggled to develop commercial models for their API and, therefore, typically only provide basic APIs to comply with regulations. In countries where banks are not required to provide APIs (some banks provide APIs, but without consistent standards) each bank’s APIs are different.

Is Government-Mandated Open Banking Successful?

There is a widespread belief that government-mandated open banking initiatives have been successful, whereas, in fact, “organic” API definition and delivery by individual banks and fintechs has often been more successful worldwide.

To illustrate this, consider the U.K. which has government-mandated open banking (U.K. Open Banking). Its published figures for August 2020 show 534 million API calls to A2A APIs. This figure is calculated across 16 bank brands. This means, on average, just over 33 million API calls to A2A APIs per bank brand per month. Considering the customer numbers for each bank, this means only a handful of API calls per customer per month. Contrast that with the volume of API calls coming from the banks’ own mobile apps, which are typically used multiple times a day to check balances and pull down transaction data, all involving multiple API calls. Therefore, although the U.K. has seen some success with government-mandated open banking, there is still some way to go.

A positive effect of government-mandated open banking is that it can include the definition of API standards. This is the case with U.K. Open Banking, along with the Berlin Group, PolishAPI, STET and SBA (for more details on these standards, see Note 2). Although certainly useful, these standards do not cover all banking use cases, since they typically focus on A2A and payments only.

Countries currently with market-driven open banking, including the U.S. and China in particular, have seen banking API growth despite a lack of government mandates. In the U.S., this has been driven by aggregators such as Plaid and Finicity who provide APIs in front of banks. Another successful U.S. open banking use case involves account opening APIs provided by banks to apps such as Uber and Airbnb so
that their customers can open bank accounts. In China, Gartner has spoken to multiple banks who have had considerable success providing loans to corporations and retail customers through API-based integration with large online e-commerce and B2B marketplaces.

Creating Banking API Products

Application leaders responsible for API programs at banks can direct their banks toward commercial API success by going beyond simple compliance with regulations. This involves the creation of API products. API products are packaged collections of APIs which serve a common business purpose, and are managed by an API product manager (for more on the role of API product manager, see The Evolving Role of the API Product Manager in Digital Product Management). API products are suited to be offered as a commercial offering.

A good example of a bank going beyond regulatory compliance with API products is ABN AMRO, that has created a banking API product called “Tikkie” for payments. Tikkie is the subject of the case study in the research note Choose the Right API Monetization and Pricing Model. The Tikkie Payment Requests API is used by service providers, both B2C and B2B, to request payments, including from within apps such as WhatsApp. The Tikkie Fast Checkout API can be used by e-commerce storefronts for check-out. ABN AMRO’s API developer portal combines APIs which conform to the European Union Payment Services Directive (PSD2), alongside API products such as Tikkie which go beyond the directive’s requirements.

Banking API Technical Standards

Banking API products can leverage technical banking API standards which are focused on specific requirements including Banking Industry Architecture Network (BIAN), identity (FAPI [financial API] — used in U.K. Open Banking and Australia’s Consumer Data Right), data sharing (FDX) and semantics (Financial Industry Business Ontology [FIBO]). These standards are described in Note 2. Unlike government-mandated open banking standards, these technical banking API standards largely come from industry. Evaluate these standards to avoid reinventing common requirements, and to align with industry best practice.

API Marketplaces

API marketplaces allow API products to be showcased together with other APIs, which may be from the same API provider or from multiple API providers. In banking, an API marketplace is often seen as the next step beyond simply providing an API developer portal. Banks providing API marketplaces include BBVA and Lloyds Banking Group, whose API marketplace is the subject of the case study in the research note How to Derive Value From APIs Using API Marketplaces.

An API marketplace is frequently built on the foundation of an API developer portal, but may also include app store capabilities (e.g., from a vendor such as AppDirect or OpenChannel) and a subscription monetization service (e.g., from a vendor such as Zuora or Aria Systems).
As API providers, application leaders responsible for API strategy at banks may create their own API marketplaces, or may register their APIs in other marketplaces. Cross-industry API marketplaces include RapidAPI and ProgrammableWeb, while banking-specific API marketplaces include Luxhub and Crosskey. API consumers may discover APIs in API marketplaces, or may simply engage with the API provider via a preexisting business relationship. This flow is shown in Figure 2 below.

Figure 2: API Marketplaces Serve Both API Consumers and API Providers

### API Marketplaces Serve Both API Consumers and API Providers

<table>
<thead>
<tr>
<th>API Providers</th>
<th>API Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can Create</td>
<td>Can Use APIs From</td>
</tr>
<tr>
<td>Can Register Their APIs in</td>
<td>Can Discover APIs in</td>
</tr>
<tr>
<td>Can Market Directly to</td>
<td>Can Directly Discover</td>
</tr>
</tbody>
</table>

Source: Gartner 733322_C

### Lightweight Governance for API Products

API products and API marketplaces should be managed by API product managers acting in a federated API platform team. An API platform team provides lightweight governance to APIs, often via automation, and is differentiated from centralized and often bureaucratic “API centers of excellence.” Citizens Bank in the U.S. has such an API team, which is profiled in the case study in Federate, Rebrand and Recharter Your API Center of Excellence to Enable an API Platform Team.

### Event-Based Banking APIs

API products providing real-time event-based or streaming API access can act as a “premium” level which goes beyond the REST request/response access used to satisfy regulatory requirements. An
example of a bank providing an event-based API product for real-time data is Standard Chartered. Using webhooks, Standard Chartered’s Notifications API product provides credit/debit notification, transaction and custody transaction statuses. Consider producing a request/response API for compliance to open banking regulations, with a productized and monetized tier providing event-based (e.g., through webhooks) or streaming (e.g., through WebSocket) access. Note, however, that event-driven APIs present a challenge for API management platforms (see The Impact of Event-Driven IT on API Management).

Incorporate API Standards Such as FDX to Provide an Alternative to Screen-Scraping

Many financial applications must connect to the bank accounts of their users. For example, a personal financial management (PFM) application which displays a customer’s overall financial health must be able to access the customer’s bank balance(s) and any loans they have. Tax preparation packages and accounting software often need to access transaction records from the customer’s bank account. In the U.S., fintech apps such as Venmo also connect to bank accounts to transfer money, which customers often prefer to be performed in real-time rather than using the batch-based Automated Clearing House (ACH) approach.

These connections between financial applications and banks are described as “account linking” because the customer links their bank account to the financial application. Banking APIs would seem to be the ideal approach for account linking. However, outside of countries with open banking mandates (shown in Figure 1), many banks do not have APIs, or have APIs that are inconsistent with each other. In counties with open banking mandates, banks may create basic APIs only for compliance, but with poor developer experience. This situation has led to the rise of banking aggregators, such as Plaid (U.S.-based, used by Venmo), Finicity (U.S.-based), TrueLayer (serving U.K. and Europe), Tink (Europewide), Belvo (serving Latin America), Brankas (serving Southeast Asia) and many others.

Banking aggregators benefit the developers of financial applications by providing a single API which abstracts the connection to multiple banks. The aggregator may use a “screen-scraping” approach to connect to the bank, whereby it logs into the bank’s web-based online banking using the customer’s credentials (typically username/password). This aggregator-based account linking and account access is shown in Figure 3 below.
The aggregator-based scenario in Figure 3 presents a number of advantages and disadvantages to the banking customer, the application provider and the bank. These are shown in Figure 4 below.
Advantages and Disadvantages of Banking API Aggregators

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account linking is straightforward, simply enter credentials in a form.</td>
<td>Any change to credentials (e.g., change of online banking password) means relinking accounts.</td>
</tr>
<tr>
<td>Only one aggregator API to use, rather than using multiple different bank APIs.</td>
<td>Difficult to switch to a different aggregator (e.g., if the current aggregator raises its API pricing).</td>
</tr>
<tr>
<td>The bank does not have to provide its own API if the aggregator “scrapes” its site.</td>
<td>Banking customer credentials are shared with the aggregator. The bank loses direct control of account access.</td>
</tr>
</tbody>
</table>

Source: Gartner 73322_C

For application leaders at smaller banks, the cost advantage of not having to provide an API may outweigh the disadvantage of losing direct control of customer access. In fact, some aggregators including Plaid (with Plaid Exchange) and Finicity offer products to banks to provide their own APIs. However, for application leaders at larger banks, which have the budget and staff to provide their own API, a consent-based approach is generally preferred over using a banking aggregator. In this approach, the customer explicitly authorizes the third-party application certain rights, such as the right to access their account balance. This requires the bank to provide a consent-management interface for their customers. This is the third step in Figure 5 below.
Figure 5: Consent-Based Open Banking API Flow

Consent-Based Open Banking API Flow

1. Customer wishes to link an application to their bank account
2. Application directs customer to the bank
3. Customer authorizes the application to access their bank account
4. Application authenticates to the bank and accesses banking data on behalf of the customer

Source: Gartner

FDX Provides a Consent-Based Alternative to Screen-Scraping

Standards are emerging for consent-based data sharing using banking APIs. In particular, the Financial Data Exchange (FDX) API specification from FS-ISAC (Financial Services Information Sharing and Analysis Center) is designed to enable secure data-sharing without screen-scraping. This specification was formerly known as the Durable Data API. FDX uses OAuth 2.0 and OpenID Connect (OIDC) to allow customers to manage access to their banking data. The Fidelity spin-off company Akoya uses FDX to allow banks to allow their customers to provide consent-based access to account data, without requiring the user to share their banking credentials with third-parties (password sharing).

When implementing consent management flows, such as the flow shown in Figure 5, beware of introducing complexity. Consent flows may be confusing to users, especially when they are redirected to their bank in order to grant consent for a third-party application. Consent management also introduces complexity for application providers who must implement complex OAuth and OIDC flows. This is one of the reasons why some banks report to Gartner that they have negotiated bilateral agreements with aggregators to allow managed access to their customers’ accounts. These bilateral agreements are tailored versions of the general-purpose API usage agreements used by banks and other API providers (for more on API usage agreements, see Quick Answer: What Should Be in an API Usage Agreement?).
Some full life cycle API management platforms provide preconfigured banking API standards as well as other inbuilt support for the associated consent flows. Critical Capabilities for Full Life Cycle API Management rates full life cycle API management vendors such as Axway, Google Apigee, IBM, MuleSoft, and WSO2 on support for the “Open Banking” use case.

**Add APIs for Real-Time Corporate Banking Integration**

The API standards shown in Figure 1 and listed in Note 1 focus on retail banking, rather than corporate banking. Gartner is frequently asked “where are the standards for corporate banking APIs?” The answer is that, because open banking regulations focus on retail banking, corporate banking API standards are lacking.

The requirements for corporate banking APIs are different, and instead typically focus on the need to move from file-based integrations to a real-time approach. The comparison between an API-based approach and file transfer is shown below (see Table 1):

**Table 1: Comparing APIs With File Transfer for Corporate Banking Integrations**

<table>
<thead>
<tr>
<th>Heading</th>
<th>APIs</th>
<th>File Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication style</td>
<td>Typically real-time but increasingly event-based (e.g., using OpenAPI Specification [OAS] 3.1 callbacks with webhooks or AsyncAPI)</td>
<td>Batch/asynchronous</td>
</tr>
<tr>
<td>Standards availability</td>
<td>Lack of widely used industry standards</td>
<td>Widespread and mature industry standards, including ISO 20022, SWIFT, ANSI X12 and FIX</td>
</tr>
<tr>
<td>Typical payload</td>
<td>JSON (for REST) or XML (SOAP) for standard interoperability</td>
<td>Fixed width for standard interoperability and transaction formats</td>
</tr>
</tbody>
</table>

Source: Gartner (November 2020)

Managed file transfer (MFT) has typically been used by banks to govern and secure file transfer in corporate banking scenarios, and with institutional clients. Rather than replacing MFT, APIs can augment MFT for banking in multiple ways. APIs can be used to drive MFT flows (“API-driven MFT”) as well as to provide real-time access to data. A blend of MFT and real-time APIs is recommended. That is because MFT remains suitable for batch processes and for large files, whereas APIs are more suited for real-time access to data and for smaller (typically up to 100K) messages.
The research note Use APIs to Modernize EDI for B2B Ecosystem Integration provides information about how APIs can augment MFT, noting that APIs do not simply replace traditional B2B integrations, but instead provide a new channel.

Finally, for credit unions, the Credit Union Financial Exchange (CUFX) standard defines specifications for exchange of data in a credit union context.

**Acronym Key and Glossary Terms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2A</td>
<td>access to accounts</td>
</tr>
<tr>
<td>BIAN</td>
<td>Banking Industry Architecture Network</td>
</tr>
<tr>
<td>FDX</td>
<td>financial data exchange</td>
</tr>
<tr>
<td>PFM</td>
<td>personal financial management</td>
</tr>
<tr>
<td>PSD2</td>
<td>Payment Services Directive</td>
</tr>
</tbody>
</table>

**Evidence**

Gartner client inquiries.

1. Are You Open Banking, Open Banking.

**Note 1: Government Approaches to Open Banking APIs**

Governments with regulatory-driven approach for banking APIs:

- **Australia** (Consumer Data Right) Consumer Data Right (CDR), Australian Competition & Consumer Commission (ACCC)
- **Brazil** (phased implementation) New Regulation on Open Banking in Brazil, Banco Central do Brasil (BCB)
- **India** (Unified Payments Interface) About UPI API, IndiaStack
- **Mexico** (Fintech Law) Law to Regulate Financial Technology Institutions
- **U.K.** (U.K. Open Banking) Open Banking Implementation Entity (OBIE) Homepage, Open Banking Implementation Entity (OBIE)

Governments encouraging banks to open APIs:

- **Bahrain** (regulatory sandbox) FinTech & Innovation, Central Bank of Bahrain (CBB)
- **Japan** (revised Banking Act) Financial Services Related Bill at the 193rd Diet
Governments currently defining their open banking API approach:

- **Canada** (Review of Open Banking)  
  Annex 3, Government of Canada
- **Malaysia** (Policy Document on Publishing Open Data using Open APIs)  
  Policy Document on Publishing Open Data Using Open API, Bank Negara Malaysia
- **Indonesia** (Working Group on standards for open APIs)  
  Bank Indonesia Urges Banking Industry to Develop Open Banking in Indonesia, Bank Indonesia
- **New Zealand** (API sandbox)  
  API Centre Homepage, API Centre
- **Nigeria** (open banking)  
  Open Technology Foundation Homepage, Open Technology Foundation
- **Russia** (regulators sandboxes)  
  Experimental Legal Regimes for Digital Innovation in the Russian Federation
- **Sri Lanka** (open banking framework)  
  Developing an Open Banking Framework for Sri Lanka, Central Bank of Sri Lanka (CBSL)

**Note 2: Examples of Banking API Standards**

Industry-driven API standards:

- **Banking Industry Architecture Network (BIAN)** — architecture focus —  
  BIAN Standards
- **OpenID Foundation (OIDF) Financial-grade API (FAPI)** — identity focus  
  Financial-Grade API — Part 1: Read-Only API Security Profile
- **Financial Data Exchange (FDX)** — secure data sharing focus  
  Financial Data Exchange (FDX) Homepage
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)** — security focus  
  Financial Services Information Sharing and Analysis Center (FS-ISAC) Homepage
- **Financial Industry Business Ontology (FIBO)** — semantics focus  
  What Is FIBO

Vendor-driven API standards:
Bank-driven API standards addressing PSD2 compliance:

- **Open Bank Project** (vendor-provided)  [API Explorer](https://openbankproject.com), Open Bank Project

**Recommended by the Authors**

- **The Evolving Role of the API Product Manager in Digital Product Management**
- **Choose the Right API Monetization and Pricing Model**
- **Gartner’s API Strategy Maturity Model**
- **How to Derive Value From APIs Using API Marketplaces**
- **Key Design Principles and Building Blocks for a Robust Digital Banking Platform**
- **How to Use KPIs to Measure the Business Value of APIs**
- **API Security: What You Need to Do to Protect Your APIs**
- **Improve the Security of Application Integration by Focusing on Identity, Data and APIs**
- **Federate, Rebrand and Recharter Your API Center of Excellence to Enable an API Platform Team**
- **Critical Capabilities for Full Life Cycle API Management**