McKinsey on Payments July 2017

Data sharing and open banking

Buzzwords like "big data" typically bring to mind quantitative exercises like the application of algorithms and analytics. While these are certainly critical steps to gaining insight, a more fundamental building block of the data market is access. Easier access to data has become a hot topic in all industries, none more so than financial services. For instance, the G20's Anti-Corruption Working Group has identified open data as a priority to advance public sector transparency and integrity. From a commercial standpoint, data can serve as a catalyst for new products and business models. The EU has been proactive on this front, setting the rules of engagement through the updated version of the Payment Services Directive (PSD2).

Laura Brodsky

Liz Oakes

Data-sharing is often accomplished through an application programming interface (API), an intelligent conduit that allows for the flow of data between systems in a controlled yet seamless fashion (Exhibit 1). APIs have been leveraged in banking settings for years (see sidebar "How open banking brings new relevance to APIs," page 20). Given breakthroughs in advanced analytics and the market traction of numerous non-bank fintech companies, however, APIs are receiving renewed attention as a means to enhance the delivery of financial services to both retail consumers and business customers.

While open banking stands to benefit end users as well as to foster innovations and new areas of competition between banks and non-banks, it is also likely to usher in an entirely new financial services ecosystem, in which banks' roles may shift markedly. It also raises issues around regulation and data privacy, which helps to explain why global markets have taken varying approaches to governance, contributing to disparate levels of progress. Regardless of region, the momentum toward open banking models seems clear, requiring banks and fintechs alike to position themselves for success in a new environment and to anticipate the likely customer impacts.

Open banking reaching a fever pitch

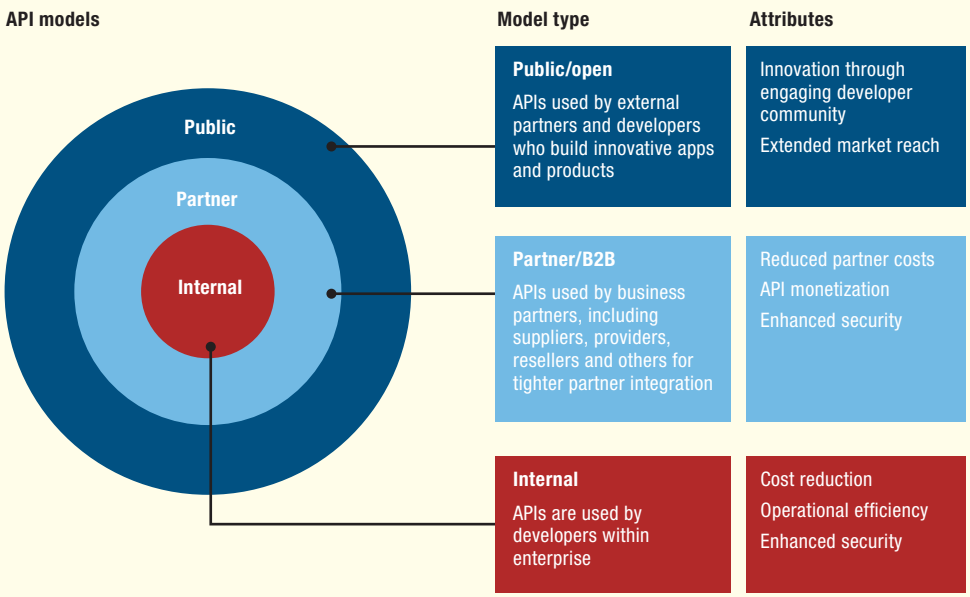
Open banking can be defined as a collaborative model in which banking data is shared through APIs between two or more unaffiliated parties to deliver enhanced capabilities to the marketplace. APIs have been used for decades, particularly in the United States, to enable personal financial management software, to present billing detail at bank websites and to connect developers to payments networks like Visa and Mastercard. To date, however, these connections have been used primarily to share information rather than to transfer monetary balances.

The potential benefits of open banking are substantial: improved customer experience, new revenue streams, and a sustainable service model for traditionally underserved markets. In addition to well-known players like Mint, examples include alternative underwriters ranging from Lending Club in the United States to M-Shwari in Africa to Lenddo in the Philippines, and payments disruptors like Stripe and Braintree (Exhibit 2, page 18).

Naturally, such advances are not quite as straightforward as our capsule description implies. Recent years have brought the development of digital ecosystems, Tencent (WeChat) and Alibaba in China being prime examples. As these ecosystems mature they begin to collide, and the inability to share data threatens to curtail innovation in business and operating models. Moreover, most advancements to date have come from firms outside the financial services realm. While incumbents still hold the keys to the vault in terms of rich transaction data as well as trusted client relationships, banks often view

Exhibit 1

Three types of APIs



Source: McKinsey Payments Practice

the opening of these data flows as more threat than opportunity. After all, it is the non-bank insurgents who have demonstrated market traction thus far, and gained valuable new customer relationships—by presenting data in new forms.

There are inherent risks in sharing data, however, which is why it is critical to develop processes and governance underpinning the technical connections. Although the core API value proposition lies in streamlining the systems integration required for data access, the need for guardrails to support protections for the privacy and security of personal data create a formidable infrastructure challenge.

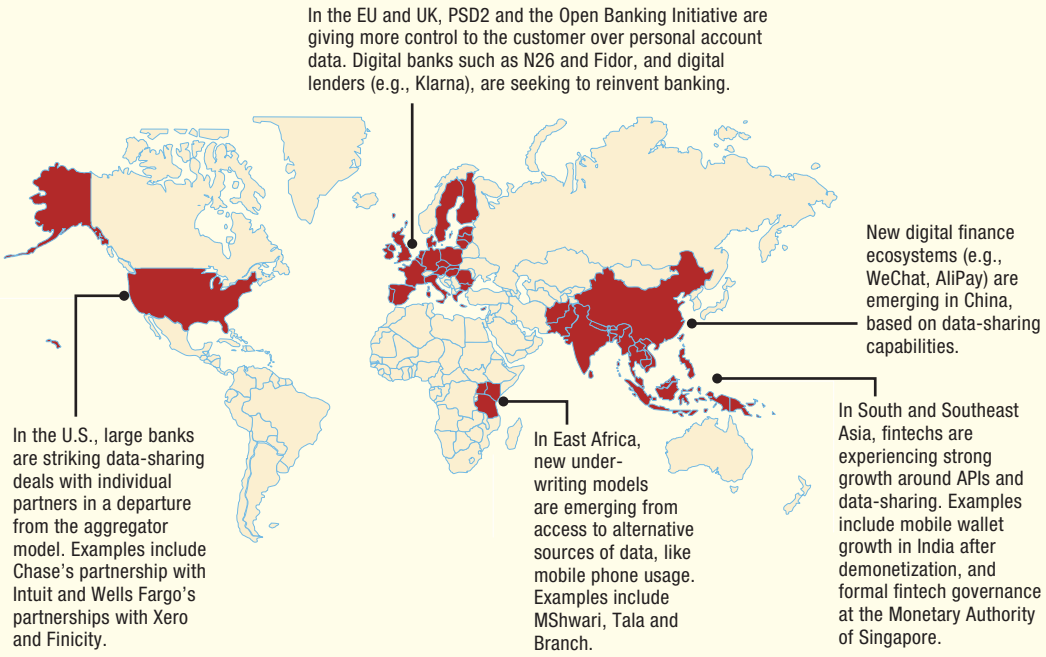
The data consent/protection elephant in the room

Notably, banks have traditionally viewed the custody and protection of their clients' data as a responsibility, more of a stewardship role than an asset to be commercialized. Data-sharing in financial services tends to be risk- and permission-based, with required audit trails, and subject to regulation and risk management. If done well, however, it can deliver increased security through enhanced know-your-customer capabilities, identity validation and fraud detection. For instance, the current version of PSD2's technical standards may put an end to the practice of screen-scraping, long a point of contention for banks.

At the same time, customer transparency and control must remain at the center of product design decisions. This is a more vexing rule to follow than it appears on the surface. Even as PSD2 is advanced by regulators, it could be argued that through

Exhibit 2

Global open-banking developments



Source: McKinsey Payments Practice

adoption consumers have already set the agenda for services they want opened to third parties. On the other hand, different data categories warrant different levels of security, and informed consent requires understanding the implications of sharing before approving—no small feat when the reflexive clicking of "I Agree" on an unread set of terms and conditions is standard. There is a fine line to walk: educating and empowering consumers without confusing, scaring or boring them.

Perhaps the most complex of these is educating end users on data permission and privacy. PSD2 explicitly empowers account holders with the authority to share data, removing the financial institution's role as gatekeeper. Further complicating matters, real-world evidence suggests consumers may not attach the same value and sensitivity to certain data elements that banks and their regulators do. Although the move to open banking need not be a zero-sum game, there are several areas where banks harbor legitimate concerns regarding loss of brand recognition and reputational risk, especially given their own required investments to effect such change.

Further questions persist regarding the duty to redact "sensitive data" in certain circumstances as well as third-party providers' obligations to delete/destroy data after a period. Many of these details remain a work in progress and will be refined as the market impacts of open banking play out. Banks are understandably concerned about such details, as any perceived disclosure missteps will almost certainly radiate back to their brand.

Another interesting twist revolves around the right to privacy. GDPR (General Data Protection Regulation), slated to take effect in the EU in May 2018, imposes a substantial penalty for noncompliance—4 percent of the offending institution's global revenues (not profits). This "right to be forgotten" significantly raises the stakes of data-sharing. Explicit consent is required from the account holder. However, there exists a silent counterparty to every financial transaction conducted by that holder; does a right to privacy exist for the corresponding payor/payee? If so, the consent process becomes infinitely more complex—particularly when parties to the transaction bank with different institutions and there is no central repository of permissions granted.

Market evolution varies by regulatory approach

Ecosystem development has varied markedly by region, due in no small part to regulatory divergence. The most programmatic approach has been taken in the EU, through both PSD2 and a broader effort to foster competition in retail banking through the UK's Open Banking Standard. A key provision of PSD2 aims to foster competition and innovation for payments service provision in the European Economic Area by opening account access to nonbanks.

The UK's pending separation from the EU is not expected to alter these data-sharing protocols, as many of PSD2's customer protection provisions are already enshrined in UK law and both the government and financial community have signaled a desire to preserve banking services compatibility—another strong indication of data-sharing's momentum. Dating back further, Italy, Belgium and Germany each instituted com-

mon protocols as early as the 1990s to provide access to account information to smaller banks and third parties.

By contrast, the absence of a centralized US approach to data governance has given rise to a series of fintech innovators as well as a patchwork of one-off bank agreements (such as partnerships struck in the US by Chase and Wells with Xero and Finicity)—a model that is not scalable in a market with roughly 12,000 financial institutions. Recently, the US Office of the Comptroller of the Currency solicited public comments regarding potential issuance of a new special purpose charter enabling fintechs to engage in limited banking functions. While the charter's intent focuses more on lending and cost of capital, it also represents a step toward making it easier for nonbanks to compete in financial services and conceivably paves the road for data-sharing protocols similar to PSD2.

India experienced remarkable fintech growth in late 2016 in the wake of the government's controversial decision to reissue fully 86 percent of its legal tender. The resulting cash shortage gave a jolt to an already growing mobile wallet segment, which is now beginning to enter a consolidation phase. Singapore has developed a large fintech market built largely around APIs, for instance, for risk-decisioning in the absence of formal credit scoring agencies. The Monetary Authority of Singapore has now established a fintech division in order to provide structure and oversight to the process. Open banking is also gaining traction in Iran (through the newly established Finnotech portal), while Australia is

How open banking brings new relevance to APIs

At its core, an API is a documented set of connecting points that allow an application to interact with another system. The concept dates back to the days of mainframe computing. Investment management firms were among the early power users, importing data on rates, fund performance, trade clearing and more from third parties onto desktop programs in a seamless fashion.

The advent of the consumer-centric internet in the early 2000s created valuable new use cases for APIs. Notably, eBay was a pioneer in sharing its APIs with approved partners who could then build out an eBay-centric ecosystem. At roughly the same time, Salesforce.com published its APIs as part of a comprehensive internet-as-a-service cloud strategy. Later in the decade, Facebook and Google Maps leveraged APIs to greatly expand the reach of their services by enlisting developers motivated to find innovative uses.

A key factor to bear in mind is that APIs can be open or proprietary. A company with the scale of Apple or Google can likely issue a set of APIs with a standard set of terms and conditions to which partners will elect to comply. Firms with less leverage, however, may face the prospect of separate, administratively onerous negotiations with a long list of potential partners.

This is why open banking has brought renewed attention to the API model. While the innovation potential of unleashing countless fintech teams to address longstanding financial services pain points is formidable, the need in a regulated industry for governance and safeguards in areas like data privacy and fiduciary responsibility is equally clear. With the aid of an oversight body—whether public or industry-led—open APIs stand to reduce the friction in bringing such solutions to market.

API software/management firms such as Plaid, Apigee, Yodlee and Xignite stand to play an integral role in open banking ecosystems. Meanwhile screen scraping—which despite material improvements remains a source of frustration for many banks—is being phased out, either by regulation or market forces delivering a more efficient solution.

considering steps mirroring those being taken by the UK and EU.

Implications for banks and new models in financial services

An open banking model can facilitate a series of services of value to both consumers and providers. Many of these exist today in some form: AliPay and WeChat enable enhanced e-commerce through their platforms, offering a smoother personalized experience and a full suite of payments options including peer-to-peer. This model can evolve to all-in-one commerce-centered apps. Services like Trustly foster the simplified extension of credit, enabling inquiries specifically at "the moment of truth," such as at checkout or elsewhere within the shopping value chain when intent has been established and a purchase decision can be influenced.

Sharing of limited data on "thin file" consumers can help to advance financial inclusion goals, pooling limited information to arrive at more precise risk-scoring and credit underwriting decisions (Angaza in Africa is an example). By introducing more consumers to the formal financial system, open banking increases the market opportunity and the potential to deliver profitable services in the future. Incubators and venture capitalists have shown particular interest in newcomers looking to incorporate non-financial data with transaction records to glean new insights—witness automated advisory service Wealthfront recently adding a lending product to its portfolio. Banks can pursue this avenue as well, from the opposite starting point.

While it seems unavoidable that open banking will result in the sacrifice of some degree of control by incumbent banks, banks will gain the offsetting benefit of participating in larger profit pools, ones in which they should be well positioned to play a leading role: for example, creating new service propositions combining predictive analytics, artificial intelligence and financing to enhance consumer and business offerings. Among incumbents, a first-mover advantage is open to organizations proactive and nimble enough to be first to deliver innovative, appealing products that customers want and need (e.g., intuitive interfaces and value-add services such as budgeting, expense categorization such as that offered by digital entrants like Monzo). The "trusted agent" status that incumbents currently enjoy will remain a competitive advantage for some time, but it must be exploited now to halt the loss of business to new entrants.

Much attention has been focused on the need for banks to open their legacy systems to APIs. However, it is equally true that Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) will need to develop interfaces to the banking market. Given that PSD2 has not defined a precise technical standard, a new category of "gateway service providers" could emerge. Google's acquisition of API management platform Apigee is an indicator of this potential, raising the stakes in a field that also includes players like Xignite and Plaid. Throughout this process, a key success factor for all parties (banks, third-party providers, and the gateways envisioned above) will be the ability to build processes that ensure security and reliability without sacrificing speed.

Banks have several strategic responses at their disposal. Although a pure go-it-alone

PSD2, GDPR and the alphabet soup of open banking

The Payment Services Directive (PSD2) is administered by the European Commission in an effort to harmonize payments regulation and consumer protections across the EU. Of particular interest in the PSD2's 2015 release (updating 2009's original directive) is an emphasis on online protections and attempts to foster marketplace innovation through open banking principles. Notwithstanding the effects of Brexit, it is believed the UK will elect to adhere to the provisions of PSD2, given the market opportunity and the fact that many of its concepts have been championed by London's financial services industry.

A key principle of the PSD2 stipulates that upon the account holder's consent, a third-party provider (TPP) must be granted access to execute instructions on the account holder's behalf. TPPs can take several forms. Account Information Service Providers (AISPs), which include offerings such as Mint in the US, are already empowered by the UK's open banking standard to deliver less sensitive information such as branch and ATM locations.

It is widely believed that enabling Payment Initiation Service Providers (PISPs) will drive significantly more innovation—and disruption—as it opens the field to actual money movement. Although Klarna and Alipay are examples of thriving PISPs, the full effect of PSD2 mandates in this area will not become apparent until their 2018 effective date (note that at the time of finalizing this article, Klarna has secured a banking license).

The UK's Open Banking Standard applies specificity to many of the principles set forth by PSD2, creating a framework for implementation including a security protocol. Effective in early 2017, the UK's nine largest retail banks were required to standardize current account and retail banking product data to permit access by registered third parties.

The General Data Protection Regulation (GDPR) is a related EU initiative aimed at unifying personal data protections across member countries. Its provisions are relevant to payments data—for both payor and payee—pursuant to "access to account" regulation. The regulation mandates data portability between processing systems; however, much-publicized "right to be forgotten" language has been softened to the "right to erasure" under many circumstances.

approach may be viable for institutions with ample resources and an agile culture, varying gradations of partnership may be a more plausible strategy. Barclays and Santander have each built open API infrastructures to deliver a virtually limitless suite of services via third-party providers (e.g., EverLedger).

Fidor and N26 are two intriguing examples of efforts to reinvent banking from the inside. Both startups are branchless institutions chartered in Germany with a fintech focus, best of breed approach, and embrace of unconventional (for banking) tactics like crowdsourcing. Their geography is likely not a coincidence, given that Germany has been called "the world's most open banking environment" by some. Fidor was acquired in 2016 by France's Groupe BPCE, but continues to operate as an independent brand.

There are ample opportunities for open banking to remake small business banking as well. A UK study found that the country's five million SMBs believe existing models offer a substandard financial service proposition. A similar sentiment would likely be found in many other countries. The UK innovation foundation Nesta has engaged to tackle this challenge, and Barclays' Pingit and Buyit solutions offer positive in-market examples.

* * *

Specific challenges will vary by geography, determined largely by the evolution of regu-

latory regimes—particularly on the private information front—and progress made to date in ecosystem development. Banks with global footprints will face particular challenges in reconciling various regions' regulations and standards (e.g., PSD2 in the EU, open banking standard in the UK, Dodd-Frank in the US) while delivering a unified service to their global customers.

Regardless of location, over the next 18 to 24 months banks should capitalize on their incumbent advantages by taking the following actions:

- Explore data-sharing agreements with fintech and non-financial services firms to stay ahead of the curve.
- Develop a perspective on APIs and their benefit to the bank's service model, both in leveraging mandated third-party access and potentially extending access beyond statutory requirements.
- Fully understand both existing data privacy mandates and likely changes, and determine their institution's appetite for a less conventional approach. And examine how customer messaging would best facilitate any such change.

Banks will need to address the potential loss of revenue from existing payments revenue streams resulting from the lowered barriers to competition. Change is rarely comfortable, but as market evolution in the United States and other countries illustrates, the forces of change are inevitable. Banks are better served getting ahead of and defining the trend rather than waging a futile battle to repel it.

Laura Brodsky *is a consultant in McKinsey's San Francisco office, and* **Liz Oakes** *is an associate partner in London.*