Draft NISTIR 8389

Cybersecurity Considerations for Open Banking Technology and Emerging Standards

Jeffrey Voas
Phil Laplante
Steve Lu
Rafail Ostrovsky
Mohamad Kassab
Nir Kshetri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8389-draft

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8389

Cybersecurity Considerations for Open Banking Technology and Emerging Standards

Jeffrey Voas
Computer Security Division
Information Technology Laboratory

Rafail Ostrovsky
UCLA
Los Angeles, CA

Phil Laplante
Mohamad Kassab
Penn State University
State College, PA

Nir Kshetri
University of North Carolina at Greensboro
Greensboro, NC

Steve Lu
Stealth Software
Los Angeles, CA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8389-draft

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8389
45 pages (January 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8389-draft

Public comment period: January 3, 2022 - March 3, 2022

Submit comments on this publication to: nistir-8389-comments@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

"Open banking" refers to a new financial ecosystem that is governed by specific security profiles, application interfaces, and guidelines with the objective of improving customer choices and experiences. Open banking ecosystems aim to provide more choices to individuals and small and mid-size businesses concerning the movement of their money, as well as information between financial institutions. Open baking also aims to make it easier for new financial service providers to enter the financial business sector. This report contains a definition and description of open banking, its activities, enablers, and cybersecurity and privacy challenges. Open banking use cases are also presented.

Keywords

open banking; computer security; privacy; cybersecurity; APIs.

Acknowledgments

The authors thank Rick Kuhn, Tom Costello, and Zubin Gautam for their input to this document.

Audience

This publication is accessible for anyone who wishes to understand open banking and the associated cybersecurity and data privacy issues. It is particularly applicable to developers of open banking standards as well as implementers of open banking applications.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nistir-8389-comments@nist.gov

Table of Contents

List of Appendices

1 Introduction

Open banking (OB) describes a new financial ecosystem that is governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations. OB ecosystems are intended to provide new choices and more information to consumers, which should allow for easier interaction with and movement of money between financial institutions and any other entity that participates in the financial ecosystem. OB also aims to make it easier for new actors to gain access to the financial sector (e.g., smaller banks and credit unions), has the potential to reduce customers fees on transactions, and is already in use in various countries.

1.1 Fundamental Banking Functions Provided by Financial Institutions

Financial institutions engage in lending, receiving deposits, and other authorized financial activities. There are nine types of financial institutions [1]: central banks, retail banks, commercial banks, credit unions, savings and loan institutions, investment banks and companies, brokerage firms, insurance companies, and mortgage companies. Central banks (e.g., the U.S. Federal Reserve Bank) only interact directly with other financial institutions. The rest of these financial institutions interact with individuals, companies, and each other in different ways. For example, banks may act as financial intermediaries by accepting customer deposits or by borrowing in the money markets. Banks then use those deposits and borrowed funds to make loans or to purchase securities. Banking entities also make loans to businesses, individuals, governments, and other entities. This document uses the term "banking entity" to refer to any financial institution that conducts business with individuals, such as a retail bank, credit union, or mortgage company. Figure 1 illustrates some monetary flows between banking entities, their customers, and other entities in the financial system.

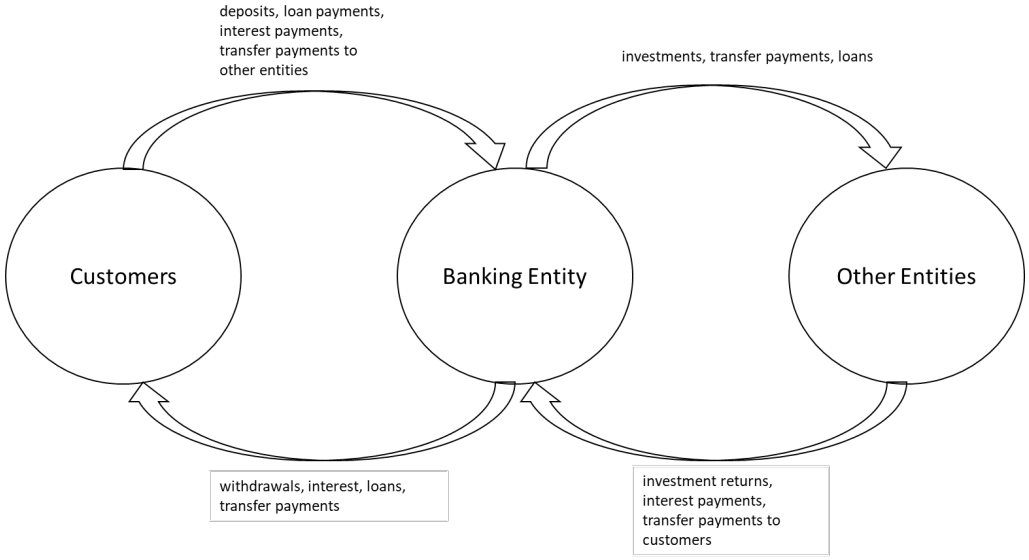


Figure 1 - Some typical interactions between banking entities, their customers, and other entities [2]

banks include individuals, merchants, service providers, governments, utilities, non-profit organizations, other banking entities, and others (e.g., consumers, investors, and businesses).

Financial sector institutions also serve as financial intermediaries by facilitating payments to and from their customers to the businesses and other entities with which they interact via check payments and debit and credit transfers. Some banking entities provide other services to their customers, such financial planning and notary services.

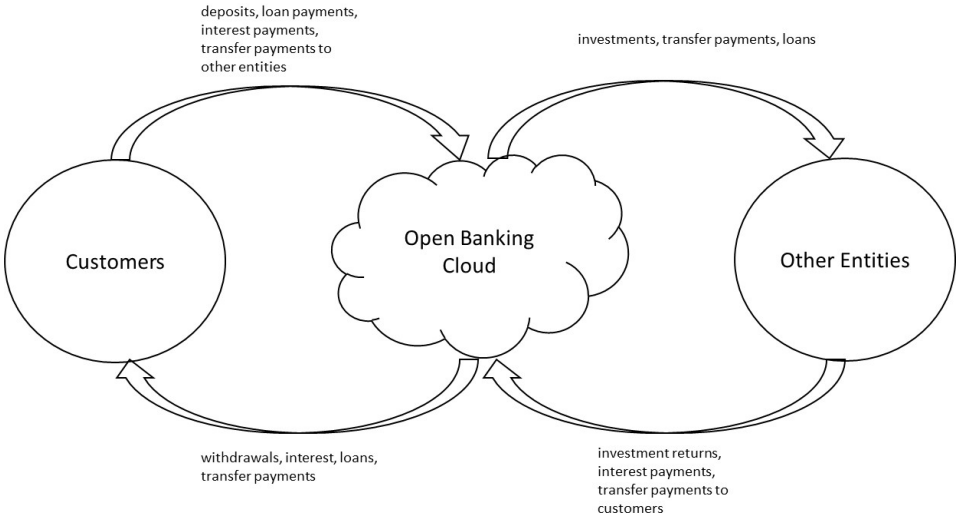
1.2 Multiple Financial Institutions

A customer can interact with more than one financial institution. For example, a person may use a local bank for everyday transactions, a credit union to hold the home mortgage, a car financing firm to finance a car, and one or more other banks for credit cards. However, moving funds between these financial institutions is not always easy or transparent. For example, making a payment to an auto loan through a credit transfer from the local bank requires several customer actions, and making a mortgage payment from an advance on a credit card requires certain authorizations.

Customers may be forced to accept most (or all) of a package of services offered by a financial institution. Customers usually cannot "mix and match" services offered by different banking entities easily. For example, it would be unusual to have a checking account with one bank, a money market account with another, a savings account with another, and debit card with yet another bank. Moving funds between these different accounts would likely require several steps and authorizations, including fees.

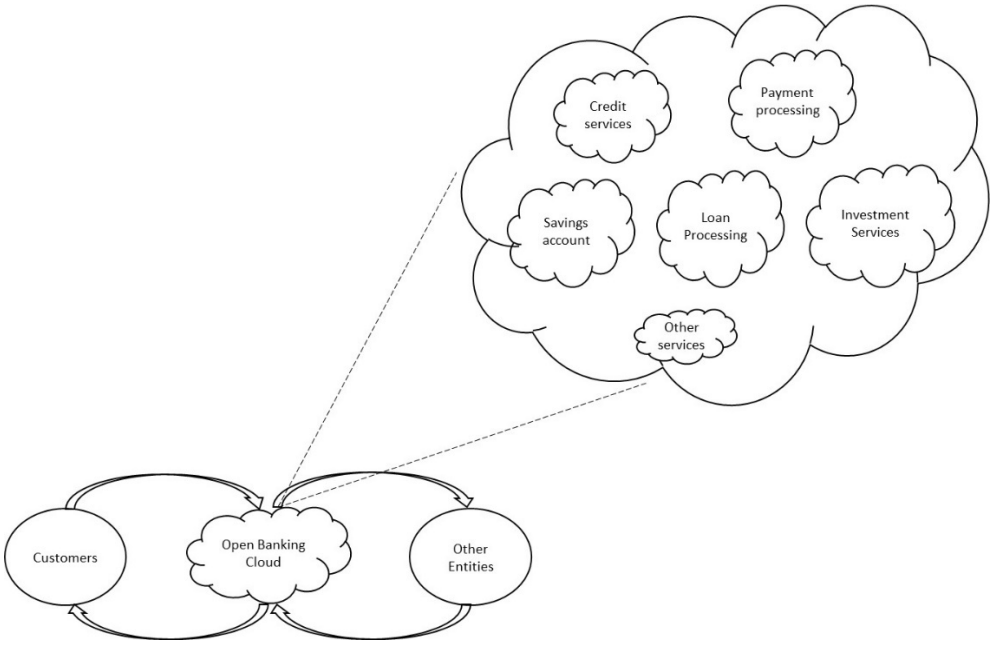
1.3 Open Banking Defined

Open banking describes a new kind of financial ecosystem that gives third-party financial service providers open access to consumer banking, transactions, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs). It is governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations. Ecosystem-enabled banking means that there are not predefined direct relationships or "supply chains" of financial products and services. Rather, the flow of debits and credits between these products and services are executed at the discretion of the customer (see Figure 2).



228

230 The term "open banking" can be used as a noun that defines any conforming financial ecosystem
231 (e.g., "the XYZ bank conducts open banking"). "Open banking" can also be used as an adjective
232 (e.g., "open banking guidelines" or "open banking API"). OB can be thought of as "finance as a
233 service" (FaaS), a form of software as a service (SaaS). In Figure 2, the open banking cloud is a
234 collection of banking entities that are configured as a cloud and deliver micro and macro
235 financial services via SaaS using conforming APIs. Financial microservices include deposits,
236 withdrawals, payments, debits, credits, and more; macro services include loan origination and
237 payoff, mortgage origination, and the like. Within the open banking cloud in Figure 2, there are
238 clouds that represent one or more financial institutions that participate in the OB ecosystem (see
239 Figure 3).



240

242 OB is consistent with the goal of moving towards a "cashless economy" by using digital
243 payments. However, it requires banks to remove proprietary barriers and share information with
244 third parties. This opening and sharing of data forces banking entities to make proprietary data
245 available to any entity with the owner's permission to access it.

246 In OB, banking entities interact with each other via APIs at the customer's direction and can
247 offer better services on an a la carte basis. With a larger available set of services, customers can
248 personalize their finances with more suitable, balanced, and cost-effective products. For
249 example, a customer could choose one banking entity's savings account service, another banking
250 entity's checking account service, another's credit card, another's auto loan, and another's
251 mortgage product, and funds could be moved seamlessly through all of these services.
252 Dashboard tools could help customers perform various transactions, aggregate information for
253 analysis and optimization, set activity alarms, and so on.

254 Aggregated accounts enable new insights and enhanced speed, convenience, and simplicity of
255 transactions. Aggregated accounts could belong to the balance sheets that clients select, or each
256 bank might only count its own accounts on its balance sheet. OB also makes it easier for smaller
257 financial product vendors to enter into the financial services industry.

2 Use Cases

Section 2 provides use cases to illustrate expected open banking experiences [3].

Use Case 1, Recurring Payments: Members of a household juggle multiple recurring payments for their mortgage, four credit cards, car insurance (insurance agency X), home insurance (insurance agency Y), life insurance (insurance agency Z), healthcare (exchange Q), property and income taxes, utilities, and much more. The household income (from three sources) appears as direct deposits into two banks. One member of the household is responsible for managing the finances. This member is finding it difficult to keep track of all of the sources of funds and has occasionally incurred costly penalties for missed and late payments and overdrafts. OB would allow the sources of income from different sources and all of the recurring expenses to be displayed on one or more dashboards that provide statuses, alerts for payment, and seamless access to funds from any source, including consolidated account overdraft protection. Aggregating this information also allows for the optimization of payment scheduling (to reduce interest charges) and the movement of money between revenue-generating accounts. Artificial intelligence can provide additional insights to optimize cashflow, minimize lateness, and lead to a higher credit rating for members of the household.

Use Case 2, Multiple Accounts: An individual has checking accounts at two different banks and a credit card financed through a third bank. The individual wishes to make large purchases that exceed the funds in any checking account or credit card limit. However, the OB allows the individual to seamlessly combine these sources into an available balance that is sufficient to make a large purchase, as well as covering shortfalls on any account as needed via direct transfers between accounts. Once the consumer makes a purchase, the checking accounts and credit card are debited accordingly.

Use Case 3, Linking Payments: A certain large banking entity no longer offers personal lines of credit but supports OB. An individual customer wishes to continue everyday business with the large bank but obtains a personal line of credit through a different banking entity that supports OB. Through OB, more seamless payment of bills from a day-to-day operational perspective is possible. For example, direct credit transfer can be used to pay the principal and interest on the line, link to the savings and checking accounts for overdraft protection on the line of credit, and transfer between accounts. These OB experiences all occur as if all accounts were held by one large bank.

Use Case 4, Auto Purchase: An individual wishes to purchase a new car from a dealer. The individual selects the particular model and options and negotiates with the dealer on the purchase price. Using OB, the auto dealer conducts a rapid credit check on the buyer, sends financial information to various loan agencies, and receives multiple loan offers and terms from various finance sources. The buyer selects the preferred loan, and the purchase down payment is directly paid to the dealer from a selected banking entity serving the customer. The payment plan is set up with a loan agency, and overdraft protection is set up by linking regular load payment sources (e.g., checking account) to other secondary financial sources (e.g., savings, investment accounts). The complete set of financial transactions takes only a few minutes.

Use Case 5, Small Business Loan Origination: A small and medium enterprise (SME) owner wishes to obtain a loan to purchase new equipment for their expanding business. The owner has been unable to get a loan from traditional banks, including their regular bank. Part of the difficulty in obtaining the loan has been the effort required to collect all of the financial information needed for the loan application while simultaneously trying to run the business. Using an OB application, however, the business owner can more easily gather the information needed for the loan applications, shop more loan sources, and select from several options in order to get the most favorable loan terms.

Use Case 6, New Banking Entities: Consider the collection of SME and large banking entities participating in the activities of Use Cases 1-5. Many of these entities would not be able to connect with nor have the opportunity to offer products and conduct business with the customers in these Use Cases without the OB ecosystem.

Use Case 7, Wealth Management: Digital wealth management platforms are on the rise and can benefit from the OB system to gain a clearer context of a client before recommending an appropriate investment based on the client's payment ability and risk tolerance. Companies that can implement this use case in the U.K. include Plum (https://withplum.com/), Chip (https://getchip.uk/), and Lenlord (https://www.lendlord.io/).

Use Case 8, Buy Now Pay Later (BNPL): A small retailer wants to implement a BNPL campaign that allows users to receive their purchased items before payments are finished. A typical step in traditional BNPL programs is determining a customer's credit risk before extending credit. This step is usually outsourced by small retailers. Using an OB framework, a specialized company can smooth the interaction between retailer and customer and reduce the burden on the retailer. OB-developed applications can aggregate more information about the customer's spending habits and use proprietary algorithms to help make a better-informed decision about the creditworthiness of a user. Companies that can implement this use case include Zilch (https://www.payzilch.com), Klarna (https://www.klarna.com), and Afterpay (https://www.afterpay.com/en-US).

Use Case 9, Improving Employee Experience: A company wants to offer its employees discount packages at retailers in their community. Typically, such a program would require proof of employment to qualify for a discount, at which time an adjustment to the retailer's point-of-sale system needs to be made. OB can streamline this process by connecting the employee's existing credit or debit card to their discount profile and unlocking eligible deals in their community. Moreover, AI capabilities can further augment the OB-developed system. By analyzing the employee's banking transactional data, the discounts can be targeted to the interests of each employee instead of a blanket discount voucher. Because there is no need to modify the vendor's system, it is also easier for a small retailer to participate in an employee discount program. Companies that can implement this use case include Perkbox (https://www.perkbox.com/uk).

Use Case 10, Debt Collection: A customer is behind on certain loan payments. Using open banking, a debt collector can look into the accounts of the person and try to generate a payment

plan that the debtor can meet to pay off the remaining amount. Companies that can implement this use case include Experian (https://www.experian.com/) and Flexys (http://flexys.com/).

Use Case 11, Carbon Tracking: An individual is interested in learning about the impact that their spending has on the environment. An OB system connected to a carbon-tracking platform can provide the user with carbon footprint insights based on their banking transactions, allowing them to become more conscious about their environmental impact. The system can also offer recommendations to engage in changing spending behaviors in a win-win ecosystem. Companies that can implement this use case include Enfuce (https://enfuce.com/) and equensWorldline (https://equensworldline.com).

3 Differences from Conventional e-Banking and Peer-To-Peer Financial Platforms

Key differences between open banking and conventional e-banking and peer-to-peer (P2P) financial platforms are presented in Table 1.

Table 1 - Comparing OB, conventional e-banking, and P2P financial platforms [2]

	Open Banking	Conventional e-Banking	P2P Financial Platforms
Privacy and security aspects	Privacy and security issues are of concern among large proportions of lenders and consumers [4].	Many are implementing strong security and privacy measures, including biometric login options involving fingerprint, voiceprint, and facial recognition [8].	Cybercriminals have been reported to use compromised identities from massive data breaches to get loans [10].
Adoption and use	Only a few jurisdictions have developed OB regulations, and the current regulatory environment has been a concern in most economies [4].	In addition to well-established e-banking services offered by existing banks, some economies such as Hong Kong SAR, South Korea, Malaysia, Singapore, Taiwan, and the Philippines have issued bespoke digital banking licenses to operate online-only banks [5].	The regulatory environment is complex and varies significantly across countries.
Potential effects on mainstream banking systems	There is the opportunity to work with FinTechs to launch innovative products and adopt ways to enhance customer experience and loyalty. With streamlined processes and new products, new customers can be gained, and existing	There are lower overhead costs than brick-and-mortar operations.	P2P loans typically offer investors a higher rate of return (albeit riskier) compared to bank deposits. Such a competition forces banks to fund their activities using more costly non-deposit funding sources [6].

	Open Banking	Conventional e-Banking	P2P Financial Platforms
	customers can be retained. However, banks may lose some income from fees.		
Potential benefits to consumers	There is access to additional products that customers' current banks cannot offer, as well as diversified access to products [7].	E-banking offers convenience (e.g., 24/7 account access) and control over finances with the ability to self-serve [8].	High-risk borrowers not served by traditional banks could get access to loans. Consumers, however, often pay higher interest rates than for loans from the traditional banking sector [9] or private lenders.

Ordinary electronic banking (e-banking) is already well-established. None of the micro or macro services provided by banks require a physical structure or proximity, and all can be conducted online. Many banking entities serve their customers entirely through online services without the need for physical branch offices. These e-banks provide capabilities for electronic deposits, the withdrawal of funds, remote scanning of physical checks for deposit, electronic transfers, auto deposits, auto debits, account analysis, transaction alerts, reminders, and more. Many conventional banks also offer an electronic interface and other third-party e-banking solutions that provide a "wrapper façade" for a mobile banking layer between the user and their bank.

However, these e-banking activities all occur within the closed system of banking entities subscribed to by a customer and are predefined and not transparent. Further, proprietary information kept by each banking entity curtails the optimization and customization of services and the consolidation of information.

P2P financial platforms (e.g., Venmo, PayPal, Google Pay) offer digital wallets with money held by the platform host and allow for transfer to and from linked debit cards, credit cards, or bank accounts depending on the service. Yet beyond the electronic wallet feature, P2P financial platforms offer few of the other services offered by traditional banks and, therefore, fall far short of the capabilities of OB. Thus, e-banking services and P2P financial networks can benefit by entering the OB ecosystem.

4 Survey of Open Banking Standards and Approaches Around the World

National approaches to open banking across the globe are frequently characterized broadly as either *regulatory* or *market-driven* [11][12]. However, the adoption of open banking in many countries might better be characterized as a hybrid approach with legal and regulatory mandates driving certain aspects of open banking and market forces driving others. This section gives a high-level survey of some national and regional approaches to open banking with a particular focus on the role that privacy and cybersecurity considerations have played in the development and implementation of these approaches.

4.1 European Union and United Kingdom

The E.U. and the U.K. have taken closely related and solidly regulatory approaches to open banking, resulting in their reputations as open banking's primary pioneers [11][13][14]. The regulatory origins of open banking in the E.U. and the U.K. can be traced to the EU's Revised Payment Services Directive (PSD2), which was adopted by the European Parliament, passed by the Council of the European Union in 2015, and came into force under EU-member national laws and regulations in early 2018 [15].

With the goal of promoting competition and innovation in the payments market, PSD2 requires Account Servicing Payment Service Providers (ASPSPs) – essentially, banks and other financial institutions (FIs) at which customers hold payment accounts – to open their payment services to regulated third-party payment service providers (TPPs) with customers' consent. These TPPs, which include FinTechs and other new players in the payments market that could also be FIs themselves, include payment initiation service providers (PISPs) and account information service providers (AISPs). PISPs provide services to initiate payments at the request of a customer using the customer's payment account held at an FI, whereas AISPs offer online services that provide consolidated information on a customer's payment accounts held at one or more FIs [15] (Article 4(15)–(19)).

More precisely, Articles 66 and 67 of PSD2 require E.U. Member States to establish and maintain the *rights* of customers to make use of services from PISPs and AISPs, respectively, and require FIs to enable those TPP services through the use of secure communications. In short, PSD2 made participation in open banking *compulsory* for FIs in the EU, which included the U.K. during the pre-Brexit time period of PSD2's enactment and coming into force, at least with respect to regulated TPPs. The U.K.'s implementation of PSD2 as the Payment Services Regulations 2017 (PSRs 2017) remains in effect, although certain post-Brexit amendments to the regulations are expected [16][17].

4.1.1 Development of Open Banking Standards and API Specifications

The U.K. has seen a somewhat more rapid implementation of OB APIs than the EU. In 2017, based on an investigation report published in August 2016, the U.K. Competition and Markets Authority (CMA) ordered the nine largest U.K. banks at the time – HSBC, Barclays, Santander, Bank of Ireland, RBS, Allied Irish Bank, Danske Bank, Nationwide, and Lloyds, collectively known as the "CMA9" – to implement common open banking standards that would allow

customers to share their banking data with licensed TPPs through the use of standardized APIs [18]. Perhaps the most notable distinguishing feature of this order is that it created a regulatorily mandated set of open banking standards, including API and security-profile specifications. Specifically, the CMA order directed the CMA9 to establish the Open Banking Implementation Entity (OBIE, also known under the trading name Open Banking Limited) – a private, non-profit entity with a steering group comprising representatives of the CMA9 banks, FinTechs, payment service providers, challenger banks, consumers, small businesses, other stakeholders, and observers from U.K. government regulators [19]. The OBIE was tasked with agreeing upon, implementing, and maintaining freely available, open, read-only, and read/write data access standards, which were to include an open API standard, data format standards, security standards, governance arrangements, and customer redress mechanisms for the read/write standard [18].

The resulting Open Banking Standard was launched in January 2018, and the expanded Version 3 was published in September 2018. Designed as a "PSD2-compliant solution ([20])," Version 3 of the U.K. Open Banking Standard includes four core components: (1) API specifications (including read/write API specifications, open data API specification, open banking directory specifications, dynamic client registration specifications, and management information (MI) reporting specifications), (2) security profiles based on the Open ID Foundation's Financial-grade API (FAPI) and Client Initiated Backchannel Authentication (CIBA) profiles, (3) customer experience guidelines, and (4) operational guidelines to support ASPSPs in requesting an exemption from PSD2 requirements to provide a so-called "contingency mechanism" in addition to Open Banking Standard-compliant APIs, as discussed further below. Although the CMA mandate requires only the CMA9 banks to comply with the Open Banking Standard, it has likely resulted in a U.K. open banking environment harmonized around clear, regulation-driven specifications. Indeed, the OBIE's monthly highlights report 91 regulated ASPSPs (presumably including the CMA9) and 234 regulated TPPs, with 114 regulated entities that "have at least one proposition live with customers" in the U.K. open banking ecosystem [21].

In contrast to the U.K.'s approach of establishing and developing concrete open banking standards through regulatory mandate, the E.U. has essentially left the task of standardization to the market [13][14]. Although PSD2 establishes a legal and regulatory framework requiring FIs and other ASPSPs to establish interoperable communications with registered TPPs, it does not provide for technical open-banking API specifications akin to the U.K.'s Open Banking Standard. Article 98 of PSD2 ("Regulatory technical standards on authentication and communication") directed the European Banking Authority (EBA) to draft regulatory technical standards (RTS) specifying, in part, "the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures" between ASPSPs, TPPs, payers, and payees. However, the resulting final draft RTS describes requirements for such "common and secure communication" at a high level and does not mention, mandate, or provide technical specifications for APIs as a prescribed or suggested communication interface. The EBA's feedback on responses from public consultation accompanying the final draft RTS note that "[t]he RTS do not mandate APIs although the EBA appreciates that the industry may agree that they are suitable" [22].

Industry consensus in the E.U. appears to have settled broadly on the use of open-banking APIs [23] despite the silence of PSD2 and the accompanying RTS on APIs. However, the lack of regulatory clarity and specific mandated technical standards has arguably impeded the development of detailed API specifications and harmonization around such specifications across the EU. Some of the more notable E.U. open banking API standards include the Berlin Group's NextGenPSD2 standard, STET's PSD2 API, Swiss Corporate API, and PolishAPI [24]. Although approximately 78 % of E.U. banks relied on the NextGenPSD2 standard as early as late 2018, the EU's environment has still been comparatively more fragmented than that of the U.K. in the early years of open banking [25][26][24]. Nonetheless, the regulatory foundation provided by PSD2 has resulted in the EU's standing as a pioneer and ongoing leader in open banking. MasterCard's Open Banking Readiness Index 2021 has recently ranked Sweden, Denmark, and Norway ahead of the U.K. for open banking readiness (owing primarily to those countries' established schemes for digital ID authentication and know-your-customer (KYC) services) [24][13]. Moreover, the Euro Retail Payments Board (ERPB) working group is set to begin work on a SEPA (single euro payments area) API Access Scheme to further the integration of the European open banking market and address business requirements, governance arrangements, and a standardized API interface [23].

4.1.2 From Open Banking to "Open Finance"

PSD2 currently provides a legal framework that regulates only the sharing of *payment* data by ASPSPs with TPPs. For example, the sharing of data related to loans, mortgages, investments, or insurance is not within the purview of the PSD2 regulations. Although the U.K. Open Banking Standard provides a regulated data-sharing framework somewhat broader than that of PSD2 – in particular by establishing procedures to allow data access to a broader range of trusted third-party entities than the licensed payment service providers covered by PSD2 – the regulatory framework for open banking across the European Economic Area and the U.K. remains largely focused on payment services. As open banking has become established in Europe, there has been a push toward a broader conception of "open finance," which would create a similar framework for the sharing of financial data beyond payment account data.

With the CMA order's implementation phase set to conclude in 2021, the banking and financial services trade association, U.K. Finance, has proposed that the OBIE be transitioned to a new industry-run services company, noting that this future entity should work to extend open banking into open finance given that "[c]ustomers do not see the relevance of the PSD2 boundary [between payment and other financial services] to their financial lives" [27][28]. Similarly, the U.K.'s Financial Conduct Authority (FCA) – a financial regulatory body independent of the U.K. government – has recently published feedback to its 2019 Call for Input on open finance, noting a "degree of consensus" among responding stakeholders that, similar to open banking, a broader open finance ecosystem would require basic elements such as a legislative and regulatory framework, common standards, and an implementation entity [29]. Calls for a transition to open finance have also occurred in the E.U. For example, in October 2020, the Berlin Group announced that it would begin work on an "openFinance API Framework" [30].

4.1.3 The Impact of Privacy and Cybersecurity Considerations

Although the E.U.'s introduction of PSD2 and the CMA's open banking efforts in the U.K. were initially motivated by a desire to increase competition and innovation in the banking and payment sectors, the E.U. and U.K. frameworks have expanded their focus to considerations of customer experience, customer data rights and control, privacy, and security. A 2018 survey by PricewaterhouseCoopers found that "the risks of data management, fraud[,] and loss of privacy" were major payment customer concerns, with 48 % of retail customers and 54 % of SMBs surveyed expressing such concerns with respect to data sharing in open banking [14].

As one aspect of addressing payment security, PSD2 and its accompanying RTS require payment service providers to apply "strong customer authentication" (SCA) – essentially amounting to multi-factor authentication – in scenarios where a payer "accesses its payment account online," "initiates an electronic payment transaction," or "carries out any action through a remote channel which may imply a risk of payment fraud or other abuses" [15] (Article 97(1)). The 3D Secure 2.0 (3DS2) protocol has emerged as the primary method for authenticating payments in compliance with PSD's SCA requirements for card-not-present transactions, though unified adoption of the protocol and national enforcement of the SCA requirement have experienced delays relative to the initial implementation timeline [31]. Additionally, payments consultancy CMSPI reported testing in September 2020 showing that 35 % of 3DS2 transactions were declined, abandoned due to customer frustration, or failed due to technical errors. At the time, CMSPI estimated that such transaction failures, if not reduced, could result in losses to European merchants exceeding €100 billion based on 2019 sales volumes [32].

Much of the technological discussion of privacy and security in OB – not only with respect to the E.U. and U.K. ecosystems but globally – has focused on the superior security of open APIs relative to the practice of screen scraping, in which customers provide their payment-account access credentials (such as username and password) directly to third-party providers who use those credentials to access and gather customers' data from an FI (or other ASPSP). Screen scraping raises security and privacy concerns for both customers – not least because the practice frequently grants a third-party access to considerably more of a customer's data than is needed for the particular service that the customer is requesting – and FIs, who can face in the event of data breaches or data misuse resulting from third-party screen scraping, even where scraping is applied without the FI's knowledge [11][14].

Notably, the RTS on Strong Customer Authentication and Common Secure Communication under PSD2 limits but does not impose an outright ban on screen scraping by TPPs. Although the RTS does effectively prohibit screen scraping as it was most frequently practiced prior to PSD2, some form of permissible screen scraping survives in the form of contingency mechanisms (alluded to in the description of the U.K. Open Banking Standard), also referred to as "fallback mechanisms." Specifically, as a compromise between the security risks of screen scraping and the potential competitive disadvantage to TPPs if an ASPSP's "dedicated interface" (*i.e.*, API) fails or is unavailable, Article 33 of the RTS requires ASPSPs to grant TPPs access to their usual customer-facing authentication and communications interfaces as part of a contingency mechanism in the event of such failure or unavailability, essentially allowing TPPs to practice screen scraping as a contingency mechanism. However, the RTS requires TPPs

utilizing such contingency measures to *identify themselves* to the relevant ASPSP prior to scraping, which theoretically mitigates some of the security risk for the ASPSP [33]. Moreover, the PSD2 RTS provides conditions under which an ASPSP could qualify for an exemption from the requirement to provide a fallback mechanism (see previous discussion of the U.K. Open Banking Standard) [34][35][36].

Even assuming the use of PSD2-compliant open APIs, significant privacy and cybersecurity concerns and attendant liability concerns necessarily remain in an open banking ecosystem premised on the sharing of individual consumers' data. In this direction, the E.U.'s General Data Protection Regulation (GDPR) ([37]) plays a crucial role alongside and beyond PSD2 in the legal and regulatory framework of the European open banking ecosystem[1].

GDPR Article 25, "Data protection by design and by default," and Article 32, "Security of processing," are of particular interest with respect to the technological aspects of privacy considerations for open banking. Article 25 may be viewed as creating a legal mandate for "data controllers" (i.e., entities that determine the purpose and means of processing individuals' personal data) to adopt both technical and organizational measures that implement the principles of "privacy by design" [39]. In the context of the PSD2 open banking framework, GDPR "data controllers" include both ASPSPs (such as FIs) and TPPs. In addition to imposing privacy by design, Article 25 requires organizations to only process personal data that are necessary for the specific purpose to be accomplished by the processing. This requirement makes explicit the application of GDPR's "data minimization" and "purpose limitation" principles to limiting the *storage* of customers' data by ASPSPs and TPPs (as well as data controllers more generally) [39]. Article 32 also requires organizations to implement technical and organizational measures "to ensure a level of security appropriate to the risk" presented by data processing, in particular from destruction, loss, alteration, unauthorized access, or disclosure of personal data that are transmitted, stored, or otherwise processed [37] (Article 32).

Notably, both Article 25 and Article 32 require organizations to "tak[e] into account the state of the art" in determining appropriate technical and organizational measures. The European Data Protection Board's Guidelines on the adoption and implementation of Article 25 further clarify that the reference to the "state of the art" obligates organizations to remain current with technological developments in privacy and security, noting that data controllers must "have knowledge of and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that *secure effective implementation* of the principles and rights of data subjects taking into account the evolving technological landscape" [40].

[1] GDPR is retained in U.K. law as the "UK GDPR," although in light of Brexit, the U.K. has independent authority to keep the regulatory framework under review. As of this writing, the post-Brexit amendments to U.K. GDPR, as reflected in the relevant "Keeling Schedule," do not include any changes to the text of Article 25 of the U.K. GDPR, which is identical to the text of Article 25 of the E.U. GDPR [38].

The GDPR data minimization and purpose limitation principles reflected in Articles 25 and 32 and the attendant liability risks for payment service providers could create an incentive for the adoption of emerging technologies that obviate the data sharing upon which open banking is currently premised. For example, certain verifications and aggregate computations commonly performed by transferring customer data from ASPSPs to TPPs through the use of open APIs could instead be performed using cryptographic techniques that do not require a TPP to access, store, or process customer data in unencrypted form at all (e.g., secure multi-party computation [SMPC], zero-knowledge proofs [ZK], private set intersections [PSI], homomorphic encryption [HE], or hardware-based solutions that rely on trusted execution environments). By reducing the amount of data shared in the open banking ecosystem in the first instance, the adoption of such technologies could ease regulatory compliance burdens and reduce liability risks for ASPSPs and TPPs. Moreover, this reduction in data sharing could provide an additional layer of protection for consumer data, reducing the need to rely on potentially inefficient post hoc regulatory enforcement remedies for consumer harm in the event of data misuse or improper exposure [41]. Particularly in light of the Article 25 and Article 32 requirements for organizations to consider the state of the art when determining and maintaining appropriate technological measures and safeguards, such cryptographic technologies could find their way into standards as their adoption increases both within the banking and financial services sectors and without.

4.2 Australia

In 2017, Australia introduced the Consumer Data Right (CDR) – an opt-in framework that grants consumers the right to direct the sharing of their data held at regulated data holder institutions (such as banks) with "accredited data recipients," or third-party service providers, through APIs [42]. The CDR is implemented by the Competition and Consumer (Consumer Data Right) Rules 2020 (CCCDR Rules), which are regulations under the legislative provisions of the Competition and Consumer Act 2010 that govern "product data requests" related to data holder institutions' products, a consumer's request for their own data, and requests for consumer data made on the consumer's behalf by an accredited third-party service provider [43]. Notably, similar to the U.K.'s adoption of the Open Banking Standard discussed above, the CDR is accompanied by the Consumer Data Standards – mandated by the CCCDR Rules and created by the Data Standards Body within the Australian Treasury – which include technical and consumer experience standards and detailed API specifications [44].

The CDR became available for sharing consumer data in July 2020 when the four major Australian banks (i.e., Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited, and Westpac Banking Corporation) were required to begin sharing consumer data for their primary brands in compliance with the CCCDR Rules and the Consumer Data Standards. An additional requirement to begin sharing consumer data for their non-primary brands was scheduled for July 2021. Other deposit-taking institutions have been required to begin sharing consumer data as of July 2021 for certain "Phase 1 products" – including basic savings, checking, debit card, and credit card accounts – with a current requirement to expand sharing to all products listed in the CCCDR Rules by February 2022 [43] [45]. The listed banking sector products for which data sharing is governed by the CCCDR Rules go beyond the basic payment services covered by PSD2 in the E.U. and the U.K. and include

certain "open finance" data, such as data for home and personal loan, mortgage, investment loan, line of credit, and retirement savings account products [43].

Participation in the CDR framework by FinTechs and other third-party service providers as accredited data recipients appears to be progressing relatively slowly. As of this writing, the Australian Government's online list of CDR providers includes only six entities as "active" data recipients – of which two are Intuit companies (Intuit Australia Pty Limited and Intuit Inc.) and two are themselves banks (Commonwealth Bank of Australia and Regional Australia Bank Ltd.) – with an additional seven currently accredited data recipients [46]. Given that the CDR does *not* prohibit screen scraping, this relatively slow adoption could be at least partially explained by third-party service providers' reluctance to submit themselves to the considerably more rigorous requirements of the CDR framework [47][48].

Despite its comparatively later rollout, Australia's CDR framework is viewed as a particularly forward-looking approach to open banking. This view is due to the primary distinguishing feature that sets the CDR apart from other countries' approaches: although it is rightly seen as providing the legal and regulatory foundation for open banking in Australia, the CDR is not limited to the banking and financial services industry at all. Rather, the CDR provides a framework for sharing consumer data across a multitude of economic sectors. The accompanying standards reflect this broad vision with a particular emphasis on establishing consistent representations of consumers across industries and a design approach focused on consumers consenting to data sharing [48]. Banking is merely the first sector to which the CDR has been applied. Next, it will be introduced to the energy sector, and subsequent application to the telecommunications sector has been proposed [49].

4.3 India

India's open banking ecosystem has been facilitated by the government-driven development of the "India Stack," a collection of APIs that combine to form a digital infrastructure comprising four technology layers [50].

(1) The "presenceless layer," controlled by the Unique Identification Authority of India (UIDAI), relies on the Aadhaar authentication system introduced by the Indian government in 2010, which is based on a 12-digit unique identity number. The Aadhaar Auth API enables digital identity verification and authentication using a consumer's 12-digit identity number to access stored biometric or demographic authentication data for comparison [51].

(2) The "paperless layer," controlled by India's Ministry of Electronics and Information Technology," facilitates the electronic storage and retrieval of documents linked to a consumer's digital identity and incorporates Aadhaar eKYC, an electronic know-your-customer service based on the aforementioned Aadhaar authentication system [52]; eSign, an API-based digital document signature service facilitated by third-party service providers licensed under India's Information Technology Act ([53]); and DigiLocker, a digital locker service that can be linked with a consumer's Aadhaar identity number or mobile number [54].

(3) The "cashless layer" is controlled by the National Payments Corporation of India (NPCI), a non-profit organization overseen by the Reserve Bank of India (RBI). A primary component of the cashless layer is an electronic payments network with interoperability between banks and third-party service providers afforded by the Unified Payments Interface (UPI), an open API standard with a standardized payments markup language [55].

(4) Finally, the "consent layer," controlled by the RBI, manages data sharing subject to a consumer's consent. A key component of the consent layer is the Data Empowerment and Protection Architecture (DEPA), a public-private effort to provide a technical and legal framework for consumers to control and consent to sharing their data. Introduced as a draft policy by the Indian Government public policy think tank NITI Aayog, the DEPA launched in the financial sector in 2020, overseen by the Ministry of Finance, RBI, and various government regulators. Similar to Australia's CDR, the DEPA framework for data sharing and consent is intended to apply beyond financial services to other sectors, including health services and telecommunications [56].

The 2020 introduction of DEPA reflects a recent focus on privacy in Indian open banking and the digital data ecosystem of the India Stack more generally. This heightened focus was perhaps motivated by early complications for the India Stack posed by privacy issues centered on the Aadhaar authentication system underlying the India Stack [55]. In particular, a series of court petitions challenging the mandatory use of the Aadhaar identification number as a violation of individual privacy rights led to a 2018 Indian Supreme Court decision that, while upholding mandatory use of Aadhaar for certain government purposes, curtailed the mandatory use of Aadhaar authentication by private entities on constitutional grounds. This decision created significant uncertainty around the legality of Aadhaar-based eKYC by banks, with some initially believing that the Supreme Court ruling had effectively banned any use of Aadhar by private companies for eKYC [57][58]. Eventually, however, the RBI allowed private banks to access the Aadhaar service for KYC purposes but with an additional requirement of customer consent to such use [59]. In response to calls for India to establish a clear legal and regulatory framework for privacy protection, the Personal Data Protection Bill was introduced in the Indian Parliament by the Ministry of Electronics and Information Technology in December 2019 [60].

Within this privacy- and consent-focused environment, the DEPA framework of the India Stack's "consent layer" can be distinguished from other open banking standards by the central role played by third-party intermediaries known as "consent managers" (CMs). In the basic DEPA model, communications by all parties related to sharing a consumer's data held at a data controller (such as a bank) with a third-party service provider (such as a FinTech) pass through the CM as an intermediary. The consumer communicates their consent to the CM, and a data request from the third-party service provider is sent to the CM, who in turn relays the request to the data controller, and – subject to the consumer's consent – the consumer's data responsive to the request is sent from the data controller to the CM to the third-party service provider using an end-to-end encrypted data flow [56]. The August 2020 version of NITI Aayog's draft policy for DEPA characterizes this reliance on CMs as a point of superiority to the U.K. Open Banking Standard, at least in the Indian open banking ecosystem, noting that the U.K.'s lack of "unbundling of the institution collecting data and the institution collecting consent … may not

work to address India's scale and diversity." The draft policy asserts that "[t]o reach [its] full population, [India] will need multiple institutions specialized in consent management innovating to provide multiple modes of obtaining informed consent (for example various form factors – audio, visual or video, or assisted with an agent)." However, it does not appear to provide a substantial explanation for why dedicated CM intermediaries, as separate parties in consent and data flows, are necessary or provide a superior model in the Indian ecosystem or in open banking more generally [61].

4.4 United States

Thus far, the approach to open banking in the United States has been almost entirely market driven. Although the U.S. has been a leading technological pioneer in many of the novel services that open banking provides – with account-aggregation FinTechs such as Yodlee, Finicity, and CashEdge (all of which have since been acquired by other entities) founded as early as 1999 – it has lagged behind other countries in developing a full-fledged open banking ecosystem.

In contrast to the heavily regulation-driven approaches of nations like the U.K., E.U. member states, and Australia and the hybrid approaches that incorporate public-private partnerships like that of India, the most significant efforts toward API-based open banking in the U.S. have come from the financial services industry itself, with participation from both FIs and FinTechs [11][62]. The Clearing House (TCH) – the U.S.'s oldest banking association owned by 24 of the largest U.S. commercial banks – has created a "model data access agreement" to streamline the negotiation of contractual data access and data sharing agreements between FIs and FinTechs [63].

From the technology side, the leading standards initiative is the Financial Data Exchange (FDX) consortium – a non-profit independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC) that seeks to "unify" the financial industry around a common, interoperable, and royalty-free standard for the secure access of user permissioned financial data," known as the FDX API [64]. In 2019, the Open Financial Exchange (OFX) consortium, the other leading industry API standardization effort at the time, joined FDX as an independent working group [65]. Although the FDX API is based on JSON data serialization [66] and the still-available OFX API employs XML serialization [67], FDX has stated that existing versions of the OFX standard will continue to be supported and that "users of OFX will have assistance to migrate to the FDX API standard" [64]. FDX's membership includes numerous FIs, FinTechs, card networks, and technology companies. Although the FDX API specification is not openly available, non-members can access the specification by registering with FDX and accepting an FDX Intellectual Property Agreement [66]. In addition to FDX, the National Automated Clearing House Association (NACHA) has established the Afinis Interoperability Standards group to advance API and other financial-service standards. Although smaller than FDX, Afinis's membership overlaps with that of FDX and includes all 12 regional banks of the U.S. Federal Reserve [68].

Preliminary efforts by the Department of the Treasury and the Consumer Financial Protection Bureau (CFPB) have provided some measure of guidance and direction for the financial services industry's efforts to develop a U.S. open banking ecosystem. In July 2018, the Treasury issued a

report – "A Financial System That Creates Economic Opportunities: Nonbank Financials, FinTech, and Innovation" – that specifically noted the significant security risks and liability burdens of screen scraping and the potential for APIs to provide a more secure method of accessing consumer financial data. Although the Treasury identified "a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping," it recommended that the best approach to such a transition for the U.S. market would involve "a solution developed by the private sector, with appropriate involvement of federal and state financial regulators" [69]. Despite the Treasury report's lack of detailed guidance, it is the only government articulation of "consumer protection principals" currently cited by FDX as part of its online FAQ in response to the question of "[w]hat federal or state regulations impact the FDX API standard" [64].

Beyond the Treasury's 2018 report, the CFPB has made some efforts to address open banking and related developments as part of its regulatory mandate to implement Section 1033 of the Dodd–Frank Wall Street Reform and Consumer Protection Act, which requires FIs to make consumers' transaction and account information available "in an electronic form usable by consumers" and is arguably the provision of U.S. legislation most salient to facilitating open banking [65]. In October 2017, the CFPB issued the "Consumer Protection Principles: Consumer-authorized financial data sharing and aggregation" report, which articulated a set of non-binding principles that were explicitly not intended to interpret or provide guidance on existing laws and regulations. These principles addressed aspects of financial data sharing including transparency; consumer access, control, and informed consent; security; dispute resolution for unauthorized access; and accountability mechanisms for risks, harms, and costs [70]. Although the CFPB Principles were not binding, the TCH Model Data Access Agreement was designed to align with the Principles [63]. In October 2020, the CFPB issued an Advance Notice of Proposed Rulemaking (ANPR) for Section 1033. The questions asked in the ANPR and the public comments addressed issues relevant to open banking, including calls in the public comments for CFPB implementation of strong privacy and security protections and for data-sharing standardization through open APIs. However, in view of the narrow scope of Section 1033, the CFPB's ability to establish an open banking ecosystem through regulatory authority remains unclear [65].

The current lack of specific guidance or standards for the U.S. has led to a degree of uncertainty in U.S. efforts to develop open banking, particularly around issues of privacy and security. For example, FIs have significant liability concerns about sharing high-risk data, such as account numbers or other personally identifiable information, as well as competitive concerns over sharing proprietary information about FI products and services, whereas account aggregators typically argue in favor of consumers' ability to decide whether or not such data are shared [12]. Moreover, in the absence of comprehensive adoption or mandated use of common API standards for the exchange of financial data, screen scraping remains prevalent in the U.S. digital financial services market [12][65]. This continued practice creates a heightened security risk for the payment ecosystem, particularly in an environment where – according to research conducted by TCH in 2019 – 80 % of consumers were unaware that they were not actually logging into their FI's website but rather providing login credentials to a TPP for the purpose of scraping [12]. Although there is a general appreciation within the U.S. financial services industry of the

benefits – even the necessity – of adopting an open banking model, the lack of clear consensus regarding how to implement such a model (whether mandated by laws and regulations or reached independently by the industry itself) has arguably been a significant obstacle to the realization of a U.S. open banking ecosystem.

4.5 Other Countries

Various countries have begun significant work towards OB. A brief summary of OB initiatives around the world is given in Table 2.

Table 2 - Summary of OB initiatives around the world

Region	OB Initiatives
Africa	• *NA*
Asia	• *2014, Singapore, Smart Nation Singapore* • *2016, India, Unified Payments Interface* • *2016, South Korea, KFTC Developer Platform* • *2016, Thailand, BOT Regulatory Sandbox* • *2017, Japan, Banking Act* • *2019, Hong Kong SAR, Open API Framework* • *2020, India, Data Empowerment and Protection Architecture* • *2020, Bahrain, Open Banking Framework*
Australia	• *2017, Australia, Consumer Data Right* • *2018, Australia, Data Sharing Compliance* • *2018, New Zealand, Payments NZ* • *2020, Australia, New Payments Platform*
Europe	• *2018, U.K., Open Banking Implementation Entity* • *2018, E.U., Payment Services Directive* • *2020, Turkey, Payment Law* • *2020, Russia, Recommendatory Standards for Open Banking*
North America	• *2018, Mexico, Fintech Law* • *2018, Canada, Consumer Directed Finance* • *2019, U.S., CFPB principles UST report*
South America	• *2019, Brazil, Open Banking Framework* • *2020, Chile, Financial Portability Act*

A brief discussion of some of these initiatives is provided below. OB efforts in the U.S. are discussed in Section 4.5.

Mexico

Led by "The Fintech Law" in 2018, the implementation of OB in Mexico serves as inspiration for other countries in Latin America. The law applies to almost all types of financial entities and both transactional and product data, but it does not cover payment operations.

Brazil

The Central Bank of Brazil has been following a phased approach in implementing the "open banking model" since it was published in 2019. It will be mandatory for large financial and banking institutions with significant international activity and optional for others. The implementation of the first phase occurred in early 2021 when the fundamental requirements for the implementation of the law were disclosed. Phase 2, in which consumers will have an option to share their data with the institutions they wish, is set to be implemented in July 2021.

Japan

Despite being among the first countries in Asia to establish its own OB framework in 2015, the measures to adopt it have been versatile and focus mostly on partnerships between banks without building API portals. For example, in 2017, three megabanks – Mizuho, Sumitomo Mitsui, and MUFG – agreed on establishing a universal QR payment system. Another milestone was recorded in 2018 when a QR code payment system called "Yoka Pay" was established as a collaborative effort between Resona Banks, Fukuoka, and Yokohama.

Singapore

The Monetary Authority of Singapore has introduced API Exchange (APIX), which provides a guidance and collaboration platform to encourage banks and TPPs to integrate and test solutions with each other via a cloud-based architecture.

Hong Kong SAR

In 2017, Hong Kong introduced the Open API Framework as part of a wider plan to move into the era of "smart banking," and it was officially published in 2018. By mid-2020, more than half of the incumbent banks had either open APIs or other OB innovations.

Russia

While still in the early stages, the Central Bank of Russia approved the first recommendatory standards for OB in 2020, which included API standards for account information, payment initiation, and information security standards. Since then, the Russian FinTech Association has been carrying out pilot projects to experiment with the standards in real settings with local banks and fintech.

Other notable initiatives

New OB initiatives are continuously developing. Recent OB regulations include the "financial Portability Act" in Chile (2020), the "Payment Law" in Turkey (2020), and the Bahrain Open Banking Framework (2020).

Other countries are letting industry lead the way. For example, Canada started government-led consultations in 2019 to examine how to build regulatory oversight for the future, but the majority of the initiatives that have been taken are industry-led. A similar story can be found in Nigeria where a group of bankers and fintech experts came together in 2017 for the OB-Nigeria initiative to drive the adoption of common API standards for the country. The OB-Nigeria API is currently under development.

5 Positive Outcomes and Risks

Since some countries have deployed their own form of OB, the approaches can be compared and the overall impacts summarized. This section focuses on the latter and provides some possible advantages and risks to implementing, adopting, fostering, and even mandating OB.

Preventing fraud. Having an open platform should stimulate the means of securing financial systems, such as by enabling better methods for detecting and preventing fraud. At a much larger scale, OB could serve as a foundation upon which measures of risk and stability can be built, thereby preventing or predicting potential weaknesses before they occur.

Risk of data leakage. Mandating, or at least fostering, adoption of OB could lead to unintended consequences. While one of the main goals of OB is to offer proper security guidelines, designs, policies, and APIs, these are ultimately implemented by the financial organizations. Organizations that are not prepared for such integration but try to hurriedly implement OB could create improperly secured endpoints that result in data leakage.

Improved consumer experience. By enabling OB, banking customers could have the capability to choose financial services across multiple financial institutions. This would attract customers to banks for specific account benefits rather than forcing them to subscribe to a large package deal. Furthermore, frontend software written by third parties can now flourish due to the existence of a common set of APIs and data standards.

Augmenting existing works. Within the U.S., there are several banking and finance APIs already in existence that serve different purposes and operate at different levels of the financial sector. An open framework, such as OB, would serve to augment and make existing frameworks more interoperable with each other and with future frameworks.

Improved sharing for marketing and insights. An open standard to both the interfaces and the standards for banking should enable much easier data sharing, shaping, and transformation. When combined with appropriate privacy and security policies, such sharing could be used by data aggregation without the overhead of building custom adapters for data import for each of their sources. This could reduce the buy-in needed to perform better marketing analytics and help galvanize academic, industry, or regulatory researchers with a better understanding of financial infrastructure.

Homogeneous systems, market competition, and walled garden versus open platforms. Security by obscurity is rarely acceptable, and much has been said about formal approaches to utilizing heterogenous systems to achieve better security. Similarly, there has long been debate about having a walled garden approach versus an open approach to technology. While market competition of services ensures that customers can get more than just a bundle deal, it also opens the possibility of inferior third-party options appearing as alternatives. Given that a fraction of today's third-party services use less accurate, less standardized, and less secure methods (such as screen scraping to gather data), having an open standard should be a net positive.

6 Software and Security Practices in Banking-Related Areas

The use of information technology within banking or financial services is not new. Electronic payment processing, payroll, transfers, and other services have long existed but are usually offered as features or benefits of a larger package deal. The controls and software mechanisms for these features are implemented in a closed manner by the institution offering the product. Most larger institutions running these services have their own security practices, and while these are generally compliant with expected modern standards, they differ greatly (e.g., online password policies between different banks). OB can improve the security of the current e-banking ecosystem by offering a set of common standards, both in software and in operational guidelines, so that large and small institutions could be held to the same level of data security.

Another popular and convenient form of banking includes P2P banking. There are many traditional forms of payment and transfer of money (e.g., cash, credit card, check, ACH, wire) that have been augmented to the point of being almost seamless for digitally sending and receiving money. These services are either adopted by, backed by, or are compatible with traditional banking services and offer customers convenient means of transferring, paying, or receiving money. An OB ecosystem would not supplant these services but rather allow them to rely on a common set of standards and APIs for handling the data so that they can focus on the true value-added features of their platforms.

While cryptocurrencies do not fall under the model of traditional banking, they nonetheless have many overlapping software and security challenges with open banking, P2P banking, and digital wallets. Many digital wallet services offer a combination of traditional banking as well as cryptocurrency features. While there are very few standards specific to this topic, they still fall under the purview of better cybersecurity practices.

Data aggregation services provide important information to consumers and institutional analysts. On the consumer side, this can span a large range of "quality of life" services, including finding the best savings or loan rate, the best features in a credit card, credit monitoring, or even financial planning. On the institutional side, aggregated data can be used in a multitude of ways, including fraud detection, customer service, forecasting and market analytics, and even advertising. Due to the large amount of data, having a common schema of data would be immensely beneficial to all parties involved, and an OB ecosystem would contribute to having such a schema. At the same time, privacy and cybersecurity are of great importance when dealing with large data. Abundant personally identifiable information and consumer habits can be valuable both in the hands of analysts and cybercriminals.

Finally, many brokerages, stock trading platforms, and automated financial planning "robo-advisors" in the U.S. already provide API access. Again, while these are not standardized, they still need to adhere to quality cybersecurity standards. However, they are also not subject to the same types of regulation as traditional banks and may therefore offer easier API access.

7 API Security: Widely Deployed Approaches and Challenges

APIs are the key element for OB success. This section first considers the classes of APIs presented in the U.K. OBIE standard: read/write, open data, directory, dynamic registration, and management reporting. Within each of these classes, some of the parallels between what has been deployed with the context of open banking, what has been deployed outside of the context of OB, and what cybersecurity challenges exist in these are considered.

7.1 Intrabank APIs

APIs are loosely separated into intrabank (namely within a single bank or financial institution) and interbank APIs. Intrabank APIs are read/write and open data. Read-only APIs provide a means to retrieve certain pieces of account information without the ability to modify it. Such APIs would be beneficial for allowing account access to a third party that only wants to gather that data to improve the experience of the customer (e.g., financial planning purposes). It provides a strong one-way flow property that prevents misuse or the malicious use of access to manipulate funds. Such APIs have been deployed in the U.S. and abroad for such settings. In contrast, read/write APIs are somewhat riskier as they allow for the modification of account data or even initiate transactions. However, carefully designed standards could readily assuage such concerns, and success stories include both international OB ecosystems as well as U.S. brokerage accounts that support API trading.

Open data standards are also important when considering API access. Having common schemas across the industry means that data can be more easily aggregated with fewer errors. Consider the example of the Australian open finance approach where data can be transmitted beyond banking and into utilities, services, and other aspects of life that involve transactions. Having such common data standards would help accelerate the development of both internal and third-party applications and promote a wider adoption of such services.

7.2 Interbank APIs

Managing accounts and identities across the ecosystem also requires an additional directory API. This requirement is akin to a public-key infrastructure where identities, certificates, keys, and such are maintained. This directory is the main entry point of APIs in order to ensure that they are authenticated, identified, and provided with appropriate identification information to perform further actions.

Critical to the management of the directory is the ability to enroll, modify, and remove entities. Although several countries have developed open banking APIs to perform such tasks, there is the complementary challenge of the physical linking between identities and people or organizations. Even in the U.S., online-only banks that do not have a brick-and-mortar presence have solutions to the problem of personal identification, but no common open standard (either in terms of software or operations) has been set. Management and reporting APIs are also important and included in the OBIE topics of focus. Having common data types, forms, and reporting contents are important for the ongoing success of deployed systems.

7.3 API Security

The U.K. OBIE uses the Open ID Foundation's Financial-grade API, which in turn uses OAuth 2.0 as a critical component. OAuth 2.0 is a protocol for user authorization and access delegation for REST endpoints. It has been widely deployed for use in web services around the world. It is by nature an open standard and serves as a solid module within an OB framework.

Another popular protocol is the single sign-on service of the Security Assertion Markup Language (SAML). SAML has not been used as much in banking services as it offers a "one-click" logon when a user has already been identified and authenticated. The convenience is also a potential weakness, especially when it comes to something as sensitive as banking data. It is nonetheless popular and secure for serving its purpose of convenient logins.

8 Privacy Relations to NIST and Other Standard Frameworks

Because banking deals with customer data, privacy is also a concern. OB initiatives should be proactive in adopting privacy frameworks, such as the NIST Privacy Framework [71], which should be considered during both the design of the OB framework as well as the adoption and integration of the framework into existing systems. In particular, the five primary functions of the NIST Privacy Framework should be observed: Identify, Govern, Control, Communicate, and Protect.

Other privacy frameworks have been adopted as well. For example, the Open ID Financial API encourages stakeholders to adhere to the ISO/IEC 29100 privacy framework [72]. The FAPI explicitly calls out 11 categories of interest: consent and choice; purpose legitimacy and specification; collection limitation; data (access) limitation; use, retention, and data disclosure limitation; accuracy and quality; openness, transparency, and notice; individual participation and access; accountability; information security; and privacy compliance.

Just as important is the OB ecosystem's ability to ensure that the data remains protected. Given the connected nature of OB, it would make sense to incorporate cybersecurity principles into the standard. Frameworks such as the NIST Cybersecurity Framework [73] provide tenets to adhere to.

Beyond traditional cybersecurity, the ability to simultaneously protect, compute, and authenticate across multiple domains has attracted the attention of new forms of cryptography. A NIST project aimed at studying multi-party and threshold cryptography is currently being offered as an approach toward distributing trust to ensure no single point of failure [74]. These new techniques can offer solutions to previously unsolved problems of computing on sensitive data and data provenance.

9 Conclusion

OB is quickly coming online with well-developed guidelines and regulations, and many countries have already implemented feasible solutions to the security and privacy problems of OB.

While the U.S. has not yet developed its own OB ecosystem, many of the necessary components already exist in e-banking and P2P services. Still, more implementation work is needed, and the experiences of other countries that are further ahead in the adoption of OB can be monitored for best practices and lessons learned regarding cybersecurity and privacy. This report has described those experiences.

Finally, this report is not intended to be a promotion of OB within the U.S but rather a factual description of the technology and how various countries have implemented it. The proposal of a specific API that would be compatible across heterogeneous systems was purposely avoided.

References

[1] Monetary and Financial Statistics Manual and Compilation Guide and Financial Soundness Indicators' Compilation Guide, International Monetary Fund, 2017. [Online]. Available at https://www.imf.org/en/Data#manuals.

[2] Phil Laplante and Nir Kshreti, "Open Banking Definition and Description." Computer, Vol. 10, October, 2021, pp. 22-28.

[3] Phil Laplante and Mohamad Kassab, "Open Banking: What it is, Where it's at, and Where it's going," Computer, January, 2022.

[4] K. Rose, "41% of lenders taking 'wait and see' approach to Open Banking" March 31, 2021. Available at https://bestadvice.co.uk/41-of-lenders-taking-wait-and-see-approach-to-open-banking/.

[5] M. Kerse & I. Jenik. "Some Countries Have Digital Bank Licenses, Others Have Digital Banks." Available at https://www.cgap.org/blog/some-countries-have-digital-bank-licenses-others-have-digital-banks.

[6] H. Farag et al., "Peer Pressure: How do Peer-to-Peer Lenders affect Banks' Cost of Deposits and Liability Structure?", 14 Jun 2019. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398843.

[7] Stan Cole. "How can banks respond to the open banking revolution?" March 30, 2021. Available at https://www.worldfinance.com/contributors/how-can-banks-respond-to-the-open-banking-revolution.

[8] M. Strohm, "5 Benefits Of Digital Banking In 2021" Feb 24, 2021. Available at https://www.forbes.com/advisor/banking/benefits-of-digital-banking/.

[9] C. de Roure et al. "How does P2P lending fit into the consumer credit market?", Deutsche Bundesbank, No 30/2016. Available at https://www.bundesbank.de/resource/blob/704046/b53dc281b4666672e6d526a35e50fd50/mL/2016-08-12-dkp-30-data.pdf.

[10] A. Najarian "Cybersecurity best practices for the booming online and P2P lending space" June 15, 2016. Available at https://www.itproportal.com/2016/06/15/cybersecurity-best-practices-for-the-booming-online-and-p2p-lending-space/.

[11] Stephen Ley et al., Deloitte. "Open Banking around the world: Towards a cross-industry data sharing ecosystem," 2018. Available at https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html.

[12] Susan M. Pandy, Federal Reserve Bank of Boston. "Modernizing U.S. Financial Services with Open Banking and APIs," February 8, 2021. Available at

https://www.bostonfed.org/-/media/Documents/PaymentStrategies/Modernizing-US-Financial-Services-with-Open-Banking-and-APIs.pdf.

[13] Alice Prahmann, Franziska Zangl, Oliver Dlugosch, and Stephanie Milcke, ndigit. "Open Banking APIs Worldwide," 2019. Available at https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf.

[14] PricewaterhouseCoopers. "The future of banking is open: How to seize the Open Banking opportunity," 2018. Available at https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf.

[15] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 2015 O.J. (L 336), p. 35–127. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366.

[16] Sidley Austin LLP. "Brexit and Payment Services: UK Proposes Amendments to Key Regulations," Sept. 18, 2018. Available at https://www.sidley.com/en/insights/newsupdates/2018/09/brexit-and-payment-services-uk-proposes-amendments-to-key-regulations.

[17] Kai Zhang, K&L Gates LLP. "Brexit: Payment Regulations on a Temporary Standstill," *National Law Review*, Volume X, Number 364, Dec. 29, 2020. Available at https://www.natlawreview.com/article/brexit-payment-regulations-temporary-standstill.

[18] Competition and Markets Authority. The Retail Banking Market Investigation Order 2017. Feb. 2, 2017. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf.

[19] Competition and Markets Authority. Explanatory Note: The Retail Banking Market Investigation Order 2017. Feb. 28, 2017. Available at https://assets.publishing.service.gov.uk/media/5ee0ec7d86650c42122f536e/retail-banking-explanatory-note.pdf.

[20] Open Banking Limited. "OBIE publishes Open Banking Standards version 3.0," Sept. 7, 2018. Available at https://www.openbanking.org.uk/news/open-banking-publishes-open-banking-standards-version-3-0/.

[21] Open Banking Limited. "The OBIE Highlights – July 2021," Aug. 19, 2021. Available at https://www.openbanking.org.uk/news/the-obie-highlights-july-2021/.

[22] European Banking Authority. Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (EBA/RTS/2017/02). Feb. 23, 2017. Available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314b

d4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf.

[23] Euro Retail Payments Board Secretariat. Mandate of the Working Group on a SEPA API Access Scheme (November 2020 – June 2021). Nov. 16, 2020. Available at https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/Mandate_of_the_working_group_on_a_SEPA_API_access_scheme.pdf?a8d9ac20cc6887d6934493dafc286d15.

[24] Alex Rolfe, Horst Forster and James Wood. "Open Banking Readiness Index: The Future of Open Banking in Europe," Payments Cards & Mobile, June 17, 2021.

[25] Eyal Sivan. "Open Banking regulation & data rights with Gavin Littlejohn," Axway Blog, July 14, 2020. Available at https://blog.axway.com/digital-strategy/open-banking-regulation-data-rights.

[26] Hakan Eroglu. "Berlin Group und der Weg zur PSD3" (in German), MoneyToday.ch, Dec. 5, 2018. Available at https://www.moneytoday.ch/news/berlin-group-und-der-weg-zur-psd3/.

[27] UK Finance. "Open Banking Futures: Blueprint and Transition Plan," March 2021. Available at https://www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-FINAL.pdf.

[28] "UK Finance sets out future model for Open Banking," Finextra, Mar. 2, 2021. Available at https://www.finextra.com/newsarticle/37583/uk-finance-sets-out-future-model-for-open-banking.

[29] Financial Conduct Authority. "FCA publishes feedback to Call for Input on open finance," Mar. 26, 2021. Available at https://www.finextra.com/newsarticle/37583/uk-finance-sets-out-future-model-for-open-banking.

[30] The Berlin Group. "PRESS RELEASE – Berlin Group starts new openFinance API Framework," Oct. 26, 2020. Available at https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework.

[31] James Roche. "Global and regional impacts of SCA and 3-D Secure 2.0 (EDS2)," The Paypers, Oct. 6, 2020. Available at https://thepaypers.com/thought-leader-insights/global-and-regional-impacts-of-sca-and-3-d-secure-20-3ds2--1244971.

[32] "SCA for PSD2 could cost merchants more than EUR 100 bln in 2021," The Paypers, Sept. 24, 2020. Available at https://thepaypers.com/digital-identity-security-online-fraud/sca-for-psd2-could-cost-merchants-more-than-eur-100-bln-in-2021--1244803.

[33] Stephen Ley and Valeria Gallo, Deloitte. "PSD2 standard on secure communication: a balancing act," 2017. Available at https://www2.deloitte.com/ie/en/pages/financial-

services/articles/psd2-standard-on-secure-communication.html.

[34] European Banking Authority. Final Report: Guidelines on the conditions to benefit from an expemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS of SCA & CSC) (EBA/GL/2018/07). Dec. 4, 2018. Available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2250578/4e3b9449-ecf9-4756-8006-cbbe74db6d03/Final%20Report%20on%20Guidelines%20on%20the%20exemption%20to%20the%20fall%20back.pdf.

[35] John Salmon and Jonathan Chertkow, Hogan Lovells. "PSD2: ban on traditional screen scraping confirmed in final strong customer authentication RTS," Nov. 29, 2017. Available at https://www.engage.hoganlovells.com/knowledgeservices/news/psd2-ban-on-traditional-screen-scraping-confirmed-in-final-strong-customer-authentication-rts.

[36] Patrice Fritsch, EY PFS Solutions. "How to navigate the fallback mechanism exemption in PSD2?" Mar. 22, 2019. Available at https://www.ey.com/en_lu/payments/psd2--navigating-the-fallback-mechanism-exemption.

[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), p. 1–88. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[38] Department for Digital Culture, Media and Sport. General Data Protection Regulation Keeling Schedule. Dec. 18, 2020. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969514/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V4.pdf.

[39] European Data Protection Supervisor. Opinion 5/2018: Preliminary Opinion on privacy by design. May 31, 2018. Available at https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[40] European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0. Oct. 20, 2020. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[41] Kenneth A. Bamberger, Ran Canetti, Shafi Goldwasser, Rebecca Wexler, and Evan Joseph Zimmerman. "Verification Dilemmas, Law, and the Promise of Zero-Knowledge Proofs," *Berkeley Technology Law Journal*, Vol. 37, No. 1 (forthcoming 2022). Preprint, May 6, 2021. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781082.

[42] Commonwealth of Australia. "What is CDR?" 2021. Available at

https://www.cdr.gov.au/what-is-cdr.

[43] Competition and Consumer (Consumer Data Right) Rules 2020. Compilation No. 3. Dec. 23, 2020. Available at https://www.legislation.gov.au/Details/F2021C00076.

[44] Data Standards Body. Consumer Data Standards. 2021. Available at https://consumerdatastandardsaustralia.github.io/standards/#introduction.

[45] Australian Competition and Consumer Commission. Compliance Guidance for Data Holders: Banking sector. April 2021. Available at https://www.accc.gov.au/system/files/CDR%20-%20Compliance%20guidance%20for%20data%20holders%20in%20the%20banking%20sector%20-%20April%202021.pdf.

[46] Commonwealth of Australia. "Current Providers," 2021. Available at https://www.cdr.gov.au/find-a-provider.

[47] Australian Competition and Consumer Commission. "Guidance on screen-scraping," Mar. 23, 2021. Available at https://cdr-support.zendesk.com/hc/en-us/articles/900005316646-Guidance-on-screen-scraping.

[48] Eyal Sivan. "Exploring data rights – an interview with James Bligh," Axway Blog, Jan. 19, 2021. Available at https://blog.axway.com/digital-strategy/james-bligh.

[49] Australian Competition and Consumer Commission. "Consumer data right (CDR)," 2021. Available at https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

[50] "About – IndiaStack." Available at https://www.indiastack.org/about/.

[51] "About Aadhaar AUTH API – IndiaStack." Available at https://www.indiastack.org/aadhaar/.

[52] "About eKYC API – IndiaStack." Available at https://www.indiastack.org/ekyc/.

[53] "About eSign API – IndiaStack." Available at https://www.indiastack.org/esign/.

[54] Digital India Corporation. "FAQs." Available at https://www.digilocker.gov.in/about/faq.

[55] Yan Carrière-Swallow, Vikram Haksar, and Manasa Patnam. "India's Approach to Open Banking: Some Implications for Financial Inclusion," IMF Working Paper WP/21/52, Feb. 26, 2021. Available at https://www.imf.org/en/Publications/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Financial-Inclusion-50049.

[56] Vikas Kathuria. "Data Empowerment and Protection Architecture: Concept and Assessment," Observer Research Foundation Issue Brief, Issue No. 487, Aug. 12, 2021.

Available at https://www.orfonline.org/research/data-empowerment-and-protection-architecture-concept-and-assessment/.

[57] Vrinda Bhandar and Rahul Narayan. "In Striking Down Section 57, SC Has Curtailed the Function Creep and Financial Future of Aadhaar," The Wire, Sept. 28, 2018. Available at https://thewire.in/law/in-striking-down-section-57-sc-has-curtailed-the-function-creep-and-financial-future-of-aadhaar.

[58] Anand Ramachandran. "The future of Aadhaar and eKYC-based solutions," The Economic Times, Mar. 4, 2019. Available at https://economictimes.indiatimes.com/small-biz/sme-sector/the-future-of-aadhar-and-ekyc-based-solutions/articleshow/68251916.cms.

[59] Srinivas Kodali. "How Private Sector Slowly Regained Access to Aadhaar Post SC Judgment," The Wire, June 14, 2019. Available at https://thewire.in/law/aadhaar-rbi-supreme-court-uidai.

[60] Rajeshwar Rao. "Open banking in India," speech, Apr. 19, 2021. Available at https://www.bis.org/review/r210419a.htm.

[61] NITI Aayog. "Data Empowerment and Protection Architecture: Draft for Discussion," Aug. 2020. Available at http://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.

[62] Eyal Sivan. "The US market-driven approach to Open Banking with Don Cardinal," Axway Blog, July 21, 2020. Available at https://blog.axway.com/amplify-products/api-management/mr-open-banking-with-don-cardinal.

[63] The Clearing House. "The Clearing House Releases Model Agreement to Help Facilitate Safe Sharing of Financial Data," Nov. 12, 2019. Available at https://www.theclearinghouse.org/payment-systems/articles/2019/11/model_agreement_press_release_11-12-19 (accessed Aug. 12, 2021).

[64] Financial Data Exchange. "Frequently Asked Questions about FDX US." Available at https://financialdataexchange.org/FDX/About/FAQ-US/FDX/About/FDX_US_FAQ.aspx.

[65] Stan Adams and John B. Morris, Jr., Center for Democracy & Technology. "Open Banking: Building Trust," May 26, 2021. Available at https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf.

[66] Financial Data Exchange. "Financial Data Exchange Launches FDX API 4.2," Nov. 10, 2020. Available at https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_FDX_API_4.2.aspx.

[67] Financial Data Exchange. OFX Banking Specification, Version 2.3. October 2020.

Available at https://www.ofx.net/downloads.html.

[68] Nacha, "Afinis Interoperability Standards." Available at https://www.nacha.org/afinis-interoperability-standards.

[69] U.S. Department of the Treasury. *A Financial System That Creates Economic Opportunities: Nonbank Financials, FinTech, and Innovation*, July 2018. Available at https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-FinTech-and-Innovation.pdf.

[70] Consumer Financial Protection Bureau. "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," Oct. 18, 2017. Available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[71] NIST. "Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0," January 2020. https://doi.org/10.6028/NIST.CSWP.01162020.

[72] "ISO/IEC 29100:2011: Information technology — Security techniques — Privacy framework," 2011.

[73] NIST. "Framework for Improving Critical Infrastructure Cybersecurity," April 2018. https://doi.org/10.6028/NIST.CSWP.04162018

[74] NIST. "Multi-Party Threshold Cryptography," 2021. Available at https://csrc.nist.gov/projects/threshold-cryptography .

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

ANPR	Advance Notice of Proposed Rulemaking
AISP	Account Information Service Provider
API	Application Programming Interface
ASPPS	Account Servicing Payment Service Providers
BNPL	Buy Now Pay Later
CFPB	Consumer Financial Protection Bureau
CIBA	Client Initiated Backchannel Authentication
CM	Consent Manager
CMA	Competition and Markets Authority (U.K.)
DEPA	Data Empowerment and Protection Architecture
e-banking	Electronic Banking
EBA	European Banking Authority (EBA)
FaaS	Finance As A Service
FAPI	Financial-Grade API
FCA	Financial Conduct Authority (U.K.)
FDX	Financial Data Exchange
FS-ISAC	Financial Services Information Sharing and Analysis Center
FI	Financial Institution
KYC	Know Your Customer
MI	Management Information
NACHA	National Automated Clearing House Association
NPCI	National Payments Corporation of India
OB	Open Banking
OBIE	Open Banking Implementation Entity (U.K.)
OFX	Open Financial Exchange
PISP	Payment Initiation Service Provider
PSD2	Revised Payment Services Directive
P2P	Peer-to-Peer

1252	RBI	Reserve Bank of India
1253	RTS	Regulatory Technical Standard
1254	SaaS	Software As A Service
1255	SAML	Security Assertion Markup Language
1256	SCA	Strong Customer Authentication
1257	SOA	Software-Oriented Architecture
1258	SEPA	Single Euro Payments Area
1259	TCH	Clearing House (TCH)
1260	TPP	Third-Party Payment Services Provider
1261	UIDAI	Unique Identification Authority of India
1262	UPI	Unified Payments Interface

Appendix B—Glossary

Aadhaar authentication	In the India banking system, the process by which a unique identifier (the Aadhaar number) along with the demographic information or biometric information of the number holder is submitted to the Central Identities Data Repository for its verification.
account servicing payment service providers	Banks and other financial institutions
banking entity	Any financial institution that conducts business with individuals, such as a retail bank, credit union, or mortgage company.
central bank	A bank that only interacts directly with other financial institutions (e.g., the U.S. Federal Reserve Bank).
consent manager	A third-party online intermediary for financial transactions.
customer	Any entity engaging in banking activities, including individuals, trusts, estates, businesses (small, mid-size, and large), other public and private entities and investors, and other banking entities.
democratization of data	Making proprietary banking information available to any entity with the owner's permission to access it.
financial ecosystem	A collection of banking entities and customers conducting financial transactions according to specific rules and governed by a particular set of laws.
FinTech	Any financial services company that primarily focuses on internet-based technology to accelerate or enhance conventional services.
open banking	A special kind of financial ecosystem governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations.