

**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>

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*

53 National Institute of Standards and Technology Interagency or Internal Report 8389
54 45 pages (January 2022)

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

57 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
58 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
59 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
60 available for the purpose.

61 There may be references in this publication to other publications currently under development by NIST in accordance
62 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
63 may be used by federal agencies even before the completion of such companion publications. Thus, until each
64 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
65 planning and transition purposes, federal agencies may wish to closely follow the development of these new
66 publications by NIST.

67 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
68 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
69 <https://csrc.nist.gov/publications>.

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

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

72 National Institute of Standards and Technology
73 Attn: Computer Security Division, Information Technology Laboratory
74 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

76

77

Reports on Computer Systems Technology

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

86

Abstract

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

95

Keywords

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

97

98

Acknowledgments

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

100

101

Audience

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

105

106

Call for Patent Claims

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

113

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

116

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

119

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

123

124 i. under reasonable terms and conditions that are demonstrably free of any unfair
125 discrimination; or

126 ii. without compensation and under reasonable terms and conditions that are
127 demonstrably free of any unfair discrimination.

128

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

134

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

137

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

139

140

141 **Table of Contents**

142 **1 Introduction 1**

143 1.1 Fundamental Banking Functions Provided by Financial Institutions 1

144 1.2 Multiple Financial Institutions 2

145 1.3 Open Banking Defined 2

146 **2 Use Cases Error! Bookmark not defined.**

147 **3 Differences from Conventional e-Banking and Peer-To-Peer Financial**

148 **Platforms 8**

149 **4 Survey of Open Banking Approaches Around the World 10**

150 4.1 European Union and United Kingdom 10

151 4.1.1 Development of open-banking standards and API specifications 10

152 4.1.2 From Open Banking to “Open Finance” 12

153 4.1.3 The Impact of Privacy and Cybersecurity Considerations 13

154 4.2 Australia 15

155 4.3 India 16

156 4.4 United States 18

157 4.5 Other Countries 20

158 **5 Positive Outcomes and Risks 23**

159 **6 Software and Security Practices in Banking-Related Areas 24**

160 **7 API Security: Widely Deployed Approaches and Challenges 25**

161 7.1 Intranbank APIs 25

162 7.2 Interbank APIs 25

163 7.3 API Security 26

164 **8 Privacy Relations to NIST and Other Standard Frameworks 27**

165 **9 Conclusion Error! Bookmark not defined.**

166 **References 29**

167 **List of Appendices**

168

169 **Appendix A— Acronyms 36**

170 **Appendix B— Glossary 38**

171

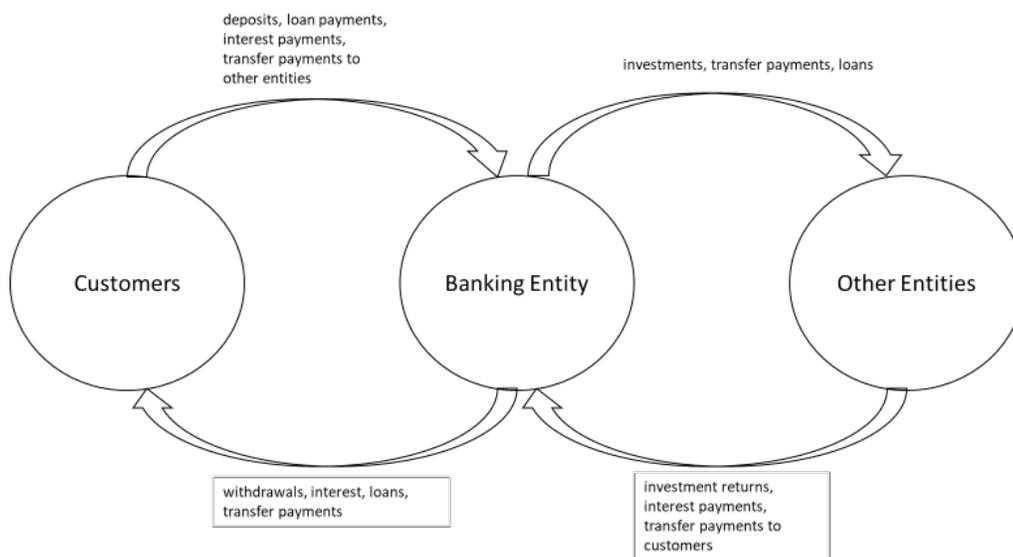
172

173 **1 Introduction**

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

181 **1.1 Fundamental Banking Functions Provided by Financial Institutions**

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



195
 196 **Figure 1 - Some typical interactions between banking entities, their customers, and other entities [2]**

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

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

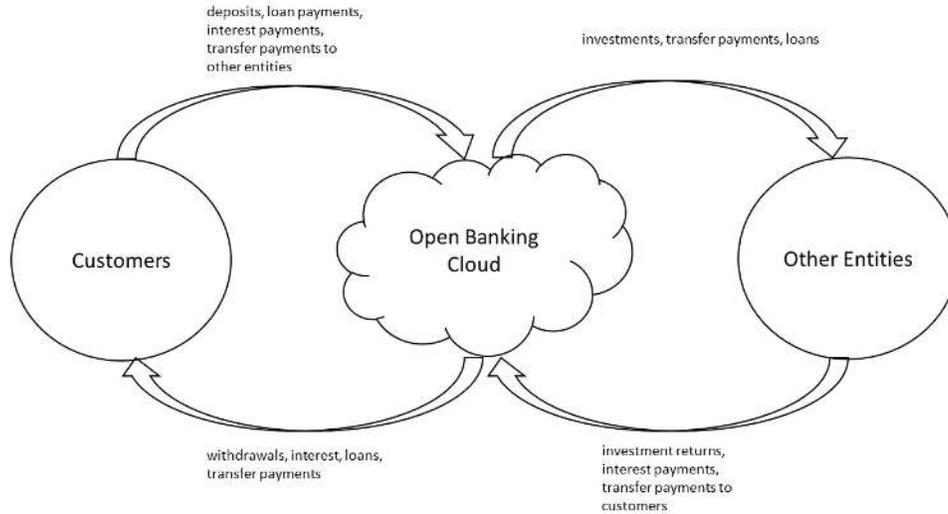
205 **1.2 Multiple Financial Institutions**

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

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

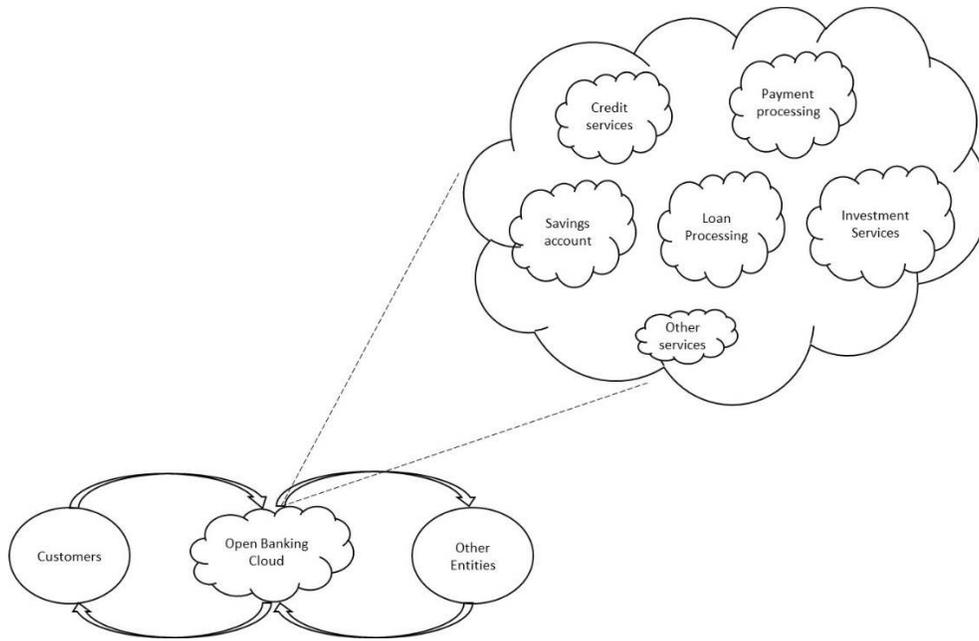
219 **1.3 Open Banking Defined**

220 Open banking describes a new kind of financial ecosystem that gives third-party financial service
221 providers open access to consumer banking, transactions, and other financial data from banks
222 and non-bank financial institutions through the use of application programming interfaces
223 (APIs). It is governed by a set of security profiles, application interfaces, and guidelines for
224 customer experiences and operations. Ecosystem-enabled banking means that there are not
225 predefined direct relationships or “supply chains” of financial products and services. Rather, the
226 flow of debits and credits between these products and services are executed at the discretion of
227 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.

258 **2 Use Cases**

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

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

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

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

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

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

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

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

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

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

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

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

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

347 **3 Differences from Conventional e-Banking and Peer-To-Peer Financial**
348 **Platforms**

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

351 **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.

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

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

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

370 **4 Survey of Open Banking Standards and Approaches Around the World**

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

378 **4.1 European Union and United Kingdom**

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

385 With the goal of promoting competition and innovation in the payments market, PSD2 requires
386 Account Servicing Payment Service Providers (ASPSPs) – essentially, banks and other financial
387 institutions (FIs) at which customers hold payment accounts – to open their payment services to
388 regulated third-party payment service providers (TPPs) with customers' consent. These TPPs,
389 which include FinTechs and other new players in the payments market that could also be FIs
390 themselves, include payment initiation service providers (PISPs) and account information service
391 providers (AISPs). PISPs provide services to initiate payments at the request of a customer using
392 the customer's payment account held at an FI, whereas AISPs offer online services that provide
393 consolidated information on a customer's payment accounts held at one or more FIs [15] (Article
394 4(15)–(19)).

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

403 **4.1.1 Development of Open Banking Standards and API Specifications**

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

409 customers to share their banking data with licensed TPPs through the use of standardized APIs
410 [18]. Perhaps the most notable distinguishing feature of this order is that it created a regulatorily
411 mandated set of open banking standards, including API and security-profile specifications.
412 Specifically, the CMA order directed the CMA9 to establish the Open Banking Implementation
413 Entity (OBIE, also known under the trading name Open Banking Limited) – a private, non-profit
414 entity with a steering group comprising representatives of the CMA9 banks, FinTechs, payment
415 service providers, challenger banks, consumers, small businesses, other stakeholders, and
416 observers from U.K. government regulators [19]. The OBIE was tasked with agreeing upon,
417 implementing, and maintaining freely available, open, read-only, and read/write data access
418 standards, which were to include an open API standard, data format standards, security
419 standards, governance arrangements, and customer redress mechanisms for the read/write
420 standard [18].

421 The resulting Open Banking Standard was launched in January 2018, and the expanded Version
422 3 was published in September 2018. Designed as a “PSD2-compliant solution ([20]),” Version 3
423 of the U.K. Open Banking Standard includes four core components: (1) API specifications
424 (including read/write API specifications, open data API specification, open banking directory
425 specifications, dynamic client registration specifications, and management information (MI)
426 reporting specifications), (2) security profiles based on the Open ID Foundation’s Financial-
427 grade API (FAPI) and Client Initiated Backchannel Authentication (CIBA) profiles, (3) customer
428 experience guidelines, and (4) operational guidelines to support ASPSPs in requesting an
429 exemption from PSD2 requirements to provide a so-called “contingency mechanism” in addition
430 to Open Banking Standard-compliant APIs, as discussed further below. Although the CMA
431 mandate requires only the CMA9 banks to comply with the Open Banking Standard, it has likely
432 resulted in a U.K. open banking environment harmonized around clear, regulation-driven
433 specifications. Indeed, the OBIE’s monthly highlights report 91 regulated ASPSPs (presumably
434 including the CMA9) and 234 regulated TPPs, with 114 regulated entities that “have at least one
435 proposition live with customers” in the U.K. open banking ecosystem [21].

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

452 Industry consensus in the E.U. appears to have settled broadly on the use of open-banking APIs
453 [23] despite the silence of PSD2 and the accompanying RTS on APIs. However, the lack of
454 regulatory clarity and specific mandated technical standards has arguably impeded the
455 development of detailed API specifications and harmonization around such specifications across
456 the EU. Some of the more notable E.U. open banking API standards include the Berlin Group’s
457 NextGenPSD2 standard, STET’s PSD2 API, Swiss Corporate API, and PolishAPI [24].
458 Although approximately 78 % of E.U. banks relied on the NextGenPSD2 standard as early as
459 late 2018, the EU’s environment has still been comparatively more fragmented than that of the
460 U.K. in the early years of open banking [25][26][24]. Nonetheless, the regulatory foundation
461 provided by PSD2 has resulted in the EU’s standing as a pioneer and ongoing leader in open
462 banking. MasterCard’s Open Banking Readiness Index 2021 has recently ranked Sweden,
463 Denmark, and Norway ahead of the U.K. for open banking readiness (owing primarily to those
464 countries’ established schemes for digital ID authentication and know-your-customer (KYC)
465 services) [24][13]. Moreover, the Euro Retail Payments Board (ERPB) working group is set to
466 begin work on a SEPA (single euro payments area) API Access Scheme to further the integration
467 of the European open banking market and address business requirements, governance
468 arrangements, and a standardized API interface [23].

469 **4.1.2 From Open Banking to “Open Finance”**

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

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

4.1.3 The Impact of Privacy and Cybersecurity Considerations

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

500 As one aspect of addressing payment security, PSD2 and its accompanying RTS require payment
501 service providers to apply “strong customer authentication” (SCA) – essentially amounting to
502 multi-factor authentication – in scenarios where a payer “accesses its payment account online,”
503 “initiates an electronic payment transaction,” or “carries out any action through a remote channel
504 which may imply a risk of payment fraud or other abuses” [15] (Article 97(1)). The 3D Secure
505 2.0 (3DS2) protocol has emerged as the primary method for authenticating payments in
506 compliance with PSD’s SCA requirements for card-not-present transactions, though unified
507 adoption of the protocol and national enforcement of the SCA requirement have experienced
508 delays relative to the initial implementation timeline [31]. Additionally, payments consultancy
509 CMSPI reported testing in September 2020 showing that 35 % of 3DS2 transactions were
510 declined, abandoned due to customer frustration, or failed due to technical errors. At the time,
511 CMSPI estimated that such transaction failures, if not reduced, could result in losses to European
512 merchants exceeding €100 billion based on 2019 sales volumes [32].

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

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

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

539 Even assuming the use of PSD2-compliant open APIs, significant privacy and cybersecurity
540 concerns and attendant liability concerns necessarily remain in an open banking ecosystem
541 premised on the sharing of individual consumers' data. In this direction, the E.U.'s General Data
542 Protection Regulation (GDPR) ([37]) plays a crucial role alongside and beyond PSD2 in the legal
543 and regulatory framework of the European open banking ecosystem¹.

544 GDPR Article 25, "Data protection by design and by default," and Article 32, "Security of
545 processing," are of particular interest with respect to the technological aspects of privacy
546 considerations for open banking. Article 25 may be viewed as creating a legal mandate for "data
547 controllers" (i.e., entities that determine the purpose and means of processing individuals'
548 personal data) to adopt both technical and organizational measures that implement the principles
549 of "privacy by design" [39]. In the context of the PSD2 open banking framework, GDPR "data
550 controllers" include both ASPSPs (such as FIs) and TPPs. In addition to imposing privacy by
551 design, Article 25 requires organizations to only process personal data that are necessary for the
552 specific purpose to be accomplished by the processing. This requirement makes explicit the
553 application of GDPR's "data minimization" and "purpose limitation" principles to limiting the
554 *storage* of customers' data by ASPSPs and TPPs (as well as data controllers more generally)
555 [39]. Article 32 also requires organizations to implement technical and organizational measures
556 "to ensure a level of security appropriate to the risk" presented by data processing, in particular
557 from destruction, loss, alteration, unauthorized access, or disclosure of personal data that are
558 transmitted, stored, or otherwise processed [37] (Article 32).

559 Notably, both Article 25 and Article 32 require organizations to "tak[e] into account the state of
560 the art" in determining appropriate technical and organizational measures. The European Data
561 Protection Board's Guidelines on the adoption and implementation of Article 25 further clarify
562 that the reference to the "state of the art" obligates organizations to remain current with
563 technological developments in privacy and security, noting that data controllers must "have
564 knowledge of and stay up to date on technological advances; how technology can present data
565 protection risks or opportunities to the processing operation; and how to implement and update
566 the measures and safeguards that *secure effective implementation* of the principles and rights of
567 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].

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

586 **4.2 Australia**

587 In 2017, Australia introduced the Consumer Data Right (CDR) – an opt-in framework that grants
588 consumers the right to direct the sharing of their data held at regulated data holder institutions
589 (such as banks) with “accredited data recipients,” or third-party service providers, through APIs
590 [42]. The CDR is implemented by the Competition and Consumer (Consumer Data Right) Rules
591 2020 (CCCDR Rules), which are regulations under the legislative provisions of the Competition
592 and Consumer Act 2010 that govern “product data requests” related to data holder institutions’
593 products, a consumer’s request for their own data, and requests for consumer data made on the
594 consumer’s behalf by an accredited third-party service provider [43]. Notably, similar to the
595 U.K.’s adoption of the Open Banking Standard discussed above, the CDR is accompanied by the
596 Consumer Data Standards – mandated by the CCCDR Rules and created by the Data Standards
597 Body within the Australian Treasury – which include technical and consumer experience
598 standards and detailed API specifications [44].

599 The CDR became available for sharing consumer data in July 2020 when the four major
600 Australian banks (i.e., Australia and New Zealand Banking Group Limited, Commonwealth
601 Bank of Australia, National Australia Bank Limited, and Westpac Banking Corporation) were
602 required to begin sharing consumer data for their primary brands in compliance with the CCCDR
603 Rules and the Consumer Data Standards. An additional requirement to begin sharing consumer
604 data for their non-primary brands was scheduled for July 2021. Other deposit-taking institutions
605 have been required to begin sharing consumer data as of July 2021 for certain “Phase 1 products”
606 – including basic savings, checking, debit card, and credit card accounts – with a current
607 requirement to expand sharing to all products listed in the CCCDR Rules by February 2022 [43]
608 [45]. The listed banking sector products for which data sharing is governed by the CCCDR Rules
609 go beyond the basic payment services covered by PSD2 in the E.U. and the U.K. and include

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

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

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

632 **4.3 India**

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

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

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

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

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

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

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

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

700 **4.4 United States**

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

706 In contrast to the heavily regulation-driven approaches of nations like the U.K., E.U. member
707 states, and Australia and the hybrid approaches that incorporate public-private partnerships like
708 that of India, the most significant efforts toward API-based open banking in the U.S. have come
709 from the financial services industry itself, with participation from both FIs and FinTechs
710 [11][62]. The Clearing House (TCH) – the U.S.’s oldest banking association owned by 24 of the
711 largest U.S. commercial banks – has created a “model data access agreement” to streamline the
712 negotiation of contractual data access and data sharing agreements between FIs and FinTechs
713 [63].

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

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

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

746 Beyond the Treasury’s 2018 report, the CFPB has made some efforts to address open banking
747 and related developments as part of its regulatory mandate to implement Section 1033 of the
748 Dodd–Frank Wall Street Reform and Consumer Protection Act, which requires FIs to make
749 consumers’ transaction and account information available “in an electronic form usable by
750 consumers” and is arguably the provision of U.S. legislation most salient to facilitating open
751 banking [65]. In October 2017, the CFPB issued the “Consumer Protection Principles:
752 Consumer-authorized financial data sharing and aggregation” report, which articulated a set of
753 non-binding principles that were explicitly not intended to interpret or provide guidance on
754 existing laws and regulations. These principles addressed aspects of financial data sharing
755 including transparency; consumer access, control, and informed consent; security; dispute
756 resolution for unauthorized access; and accountability mechanisms for risks, harms, and costs
757 [70]. Although the CFPB Principles were not binding, the TCH Model Data Access Agreement
758 was designed to align with the Principles [63]. In October 2020, the CFPB issued an Advance
759 Notice of Proposed Rulemaking (ANPR) for Section 1033. The questions asked in the ANPR
760 and the public comments addressed issues relevant to open banking, including calls in the public
761 comments for CFPB implementation of strong privacy and security protections and for data-
762 sharing standardization through open APIs. However, in view of the narrow scope of Section
763 1033, the CFPB’s ability to establish an open banking ecosystem through regulatory authority
764 remains unclear [65].

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

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

782 4.5 Other Countries

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

785 **Table 2 - Summary of OB initiatives around the world**

Region	OB Initiatives
Africa	<ul style="list-style-type: none"> • <i>NA</i>
Asia	<ul style="list-style-type: none"> • <i>2014, Singapore, Smart Nation Singapore</i> • <i>2016, India, Unified Payments Interface</i> • <i>2016, South Korea, KFTC Developer Platform</i> • <i>2016, Thailand, BOT Regulatory Sandbox</i> • <i>2017, Japan, Banking Act</i> • <i>2019, Hong Kong SAR, Open API Framework</i> • <i>2020, India, Data Empowerment and Protection Architecture</i> • <i>2020, Bahrain, Open Banking Framework</i>
Australia	<ul style="list-style-type: none"> • <i>2017, Australia, Consumer Data Right</i> • <i>2018, Australia, Data Sharing Compliance</i> • <i>2018, New Zealand, Payments NZ</i> • <i>2020, Australia, New Payments Platform</i>
Europe	<ul style="list-style-type: none"> • <i>2018, U.K., Open Banking Implementation Entity</i> • <i>2018, E.U., Payment Services Directive</i> • <i>2020, Turkey, Payment Law</i> • <i>2020, Russia, Recommendatory Standards for Open Banking</i>
North America	<ul style="list-style-type: none"> • <i>2018, Mexico, Fintech Law</i> • <i>2018, Canada, Consumer Directed Finance</i> • <i>2019, U.S., CFPB principles UST report</i>
South America	<ul style="list-style-type: none"> • <i>2019, Brazil, Open Banking Framework</i> • <i>2020, Chile, Financial Portability Act</i>

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

788 *Mexico*

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

792 *Brazil*

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

799 *Japan*

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

806 *Singapore*

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

810 *Hong Kong SAR*

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

814 *Russia*

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

820 *Other notable initiatives*

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

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

5 Positive Outcomes and Risks

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

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

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

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

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

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

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

6 Software and Security Practices in Banking-Related Areas

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

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

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

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

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

904 **7 API Security: Widely Deployed Approaches and Challenges**

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

910 **7.1 Intrabank APIs**

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

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

928 **7.2 Interbank APIs**

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

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

942 **7.3 API Security**

943 The U.K. OBIE uses the Open ID Foundation’s Financial-grade API, which in turn uses OAuth
944 2.0 as a critical component. OAuth 2.0 is a protocol for user authorization and access delegation
945 for REST endpoints. It has been widely deployed for use in web services around the world. It is
946 by nature an open standard and serves as a solid module within an OB framework.

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

8 Privacy Relations to NIST and Other Standard Frameworks

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

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

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

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

975 9 Conclusion

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

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

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

987 **References**

- 988 [1] Monetary and Financial Statistics Manual and Compilation Guide and Financial
989 Soundness Indicators' Compilation Guide, International Monetary Fund, 2017. [Online].
990 Available at <https://www.imf.org/en/Data#manuals>.
- 991 [2] Phil Laplante and Nir Kshreti, "Open Banking Definition and Description." Computer,
992 Vol. 10, October, 2021, pp. 22-28.
- 993 [3] Phil Laplante and Mohamad Kassab, "Open Banking: What it is, Where it's at, and
994 Where it's going," Computer, January, 2022.
- 995 [4] K. Rose, "41% of lenders taking 'wait and see' approach to Open Banking" March 31,
996 2021. Available at [https://bestadvice.co.uk/41-of-lenders-taking-wait-and-see-approach-
997 to-open-banking/](https://bestadvice.co.uk/41-of-lenders-taking-wait-and-see-approach-to-open-banking/).
- 998 [5] M. Kerse & I. Jenik. "Some Countries Have Digital Bank Licenses, Others Have Digital
999 Banks." Available at [https://www.cgap.org/blog/some-countries-have-digital-bank-
1000 licenses-others-have-digital-banks](https://www.cgap.org/blog/some-countries-have-digital-bank-licenses-others-have-digital-banks).
- 1001 [6] H. Farag et al., "Peer Pressure: How do Peer-to-Peer Lenders affect Banks' Cost of
1002 Deposits and Liability Structure?", 14 Jun 2019. Available at
1003 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398843.
- 1004 [7] Stan Cole. "How can banks respond to the open banking revolution?" March 30, 2021.
1005 Available at [https://www.worldfinance.com/contributors/how-can-banks-respond-to-the-
1006 open-banking-revolution](https://www.worldfinance.com/contributors/how-can-banks-respond-to-the-open-banking-revolution).
- 1007 [8] M. Strohm, "5 Benefits Of Digital Banking In 2021" Feb 24, 2021. Available at
1008 <https://www.forbes.com/advisor/banking/benefits-of-digital-banking/>.
- 1009 [9] C. de Roure et al. "How does P2P lending fit into the consumer credit market?",
1010 Deutsche Bundesbank, No 30/2016. Available at
1011 [https://www.bundesbank.de/resource/blob/704046/b53dc281b4666672e6d526a35e50fd5
1012 0/mL/2016-08-12-dkp-30-data.pdf](https://www.bundesbank.de/resource/blob/704046/b53dc281b4666672e6d526a35e50fd50/mL/2016-08-12-dkp-30-data.pdf).
- 1013 [10] A. Najarian "Cybersecurity best practices for the booming online and P2P lending space"
1014 June 15, 2016. Available at [https://www.itproportal.com/2016/06/15/cybersecurity-best-
1015 practices-for-the-booming-online-and-p2p-lending-space/](https://www.itproportal.com/2016/06/15/cybersecurity-best-practices-for-the-booming-online-and-p2p-lending-space/).
- 1016 [11] Stephen Ley et al., Deloitte. "Open Banking around the world: Towards a cross-industry
1017 data sharing ecosystem," 2018. Available at
1018 [https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-
1019 around-the-world.html](https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html).
- 1020 [12] Susan M. Pandey, Federal Reserve Bank of Boston. "Modernizing U.S. Financial Services
1021 with Open Banking and APIs," February 8, 2021. Available at

- 1022 [https://www.bostonfed.org/-/media/Documents/PaymentStrategies/Modernizing-US-](https://www.bostonfed.org/-/media/Documents/PaymentStrategies/Modernizing-US-Financial-Services-with-Open-Banking-and-APIs.pdf)
1023 [Financial-Services-with-Open-Banking-and-APIs.pdf](https://www.bostonfed.org/-/media/Documents/PaymentStrategies/Modernizing-US-Financial-Services-with-Open-Banking-and-APIs.pdf).
- 1024 [13] Alice Prahmann, Franziska Zangl, Oliver Dlugosch, and Stephanie Milcke, ndigit. “Open
1025 Banking APIs Worldwide,” 2019. Available at [https://www.openbankingexpo.com/wp-](https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf)
1026 [content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf](https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf).
- 1027 [14] PricewaterhouseCoopers. “The future of banking is open: How to seize the Open
1028 Banking opportunity,” 2018. Available at [https://www.pwc.co.uk/financial-](https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf)
1029 [services/assets/open-banking-report-web-interactive.pdf](https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf).
- 1030 [15] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25
1031 November 2015 on payment services in the internal market, amending Directives
1032 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and
1033 repealing Directive 2007/64/EC, 2015 O.J. (L 336), p. 35–127. Available at [https://eur-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366)
1034 [lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366).
- 1035 [16] Sidley Austin LLP. “Brexit and Payment Services: UK Proposes Amendments to Key
1036 Regulations,” Sept. 18, 2018. Available at
1037 [https://www.sidley.com/en/insights/newsupdates/2018/09/brexit-and-payment-services-](https://www.sidley.com/en/insights/newsupdates/2018/09/brexit-and-payment-services-uk-proposes-amendments-to-key-regulations)
1038 [uk-proposes-amendments-to-key-regulations](https://www.sidley.com/en/insights/newsupdates/2018/09/brexit-and-payment-services-uk-proposes-amendments-to-key-regulations).
- 1039 [17] Kai Zhang, K&L Gates LLP. “Brexit: Payment Regulations on a Temporary Standstill,”
1040 *National Law Review*, Volume X, Number 364, Dec. 29, 2020. Available at
1041 <https://www.natlawreview.com/article/brexit-payment-regulations-temporary-standstill>.
- 1042 [18] Competition and Markets Authority. The Retail Banking Market Investigation Order
1043 2017. Feb. 2, 2017. Available at
1044 [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf)
1045 [data/file/600842/retail-banking-market-investigation-order-2017.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf).
- 1046 [19] Competition and Markets Authority. Explanatory Note: The Retail Banking Market
1047 Investigation Order 2017. Feb. 28, 2017. Available at
1048 [https://assets.publishing.service.gov.uk/media/5ee0ec7d86650c42122f536e/retail-](https://assets.publishing.service.gov.uk/media/5ee0ec7d86650c42122f536e/retail-banking-explanatory-note.pdf)
1049 [banking-explanatory-note.pdf](https://assets.publishing.service.gov.uk/media/5ee0ec7d86650c42122f536e/retail-banking-explanatory-note.pdf).
- 1050 [20] Open Banking Limited. “OBIE publishes Open Banking Standards version 3.0,” Sept. 7,
1051 2018. Available at [https://www.openbanking.org.uk/news/open-banking-publishes-open-](https://www.openbanking.org.uk/news/open-banking-publishes-open-banking-standards-version-3-0/)
1052 [banking-standards-version-3-0/](https://www.openbanking.org.uk/news/open-banking-publishes-open-banking-standards-version-3-0/).
- 1053 [21] Open Banking Limited. “The OBIE Highlights – July 2021,” Aug. 19, 2021. Available at
1054 <https://www.openbanking.org.uk/news/the-obie-highlights-july-2021/>.
- 1055 [22] European Banking Authority. Final Report: Draft Regulatory Technical Standards on
1056 Strong Customer Authentication and common and secure communication under Article
1057 98 of Directive 2015/2366 (PSD2) (EBA/RTS/2017/02). Feb. 23, 2017. Available at
1058 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314b>

- 1059 [d4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf](https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf).
- 1060
- 1061
- 1062 [23] Euro Retail Payments Board Secretariat. Mandate of the Working Group on a SEPA API
1063 Access Scheme (November 2020 – June 2021). Nov. 16, 2020. Available at
1064 [https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-
1065 meeting/Mandate_of_the_working_group_on_a_SEPA_API_access_scheme.pdf?a8d9ac
1066 20cc6887d6934493dafc286d15](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).
- 1067 [24] Alex Rolfe, Horst Forster and James Wood. “Open Banking Readiness Index: The Future
1068 of Open Banking in Europe,” Payments Cards & Mobile, June 17, 2021.
- 1069 [25] Eyal Sivan. “Open Banking regulation & data rights with Gavin Littlejohn,” Axway
1070 Blog, July 14, 2020. Available at [https://blog.axway.com/digital-strategy/open-banking-
1071 regulation-data-rights](https://blog.axway.com/digital-strategy/open-banking-regulation-data-rights).
- 1072 [26] Hakan Eroglu. “Berlin Group und der Weg zur PSD3” (in German), MoneyToday.ch,
1073 Dec. 5, 2018. Available at [https://www.moneytoday.ch/news/berlin-group-und-der-weg-
1074 zur-psd3/](https://www.moneytoday.ch/news/berlin-group-und-der-weg-zur-psd3/).
- 1075 [27] UK Finance. “Open Banking Futures: Blueprint and Transition Plan,” March 2021.
1076 Available at [https://www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-
1077 FINAL.pdf](https://www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-FINAL.pdf).
- 1078 [28] “UK Finance sets out future model for Open Banking,” Finextra, Mar. 2, 2021. Available
1079 at [https://www.finextra.com/newsarticle/37583/uk-finance-sets-out-future-model-for-
1080 open-banking](https://www.finextra.com/newsarticle/37583/uk-finance-sets-out-future-model-for-open-banking).
- 1081 [29] Financial Conduct Authority. “FCA publishes feedback to Call for Input on open
1082 finance,” Mar. 26, 2021. Available at [https://www.finextra.com/newsarticle/37583/uk-
1083 finance-sets-out-future-model-for-open-banking](https://www.finextra.com/newsarticle/37583/uk-finance-sets-out-future-model-for-open-banking).
- 1084 [30] The Berlin Group. “PRESS RELEASE – Berlin Group starts new openFinance API
1085 Framework,” Oct. 26, 2020. Available at [https://www.berlin-group.org/single-post/press-
1086 release-berlin-group-starts-new-openfinance-api-framework](https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework).
- 1087 [31] James Roche. “Global and regional impacts of SCA and 3-D Secure 2.0 (EDS2),” The
1088 Paypers, Oct. 6, 2020. Available at [https://thepayers.com/thought-leader-insights/global-
1089 and-regional-impacts-of-sca-and-3-d-secure-20-3ds2--1244971](https://thepayers.com/thought-leader-insights/global-and-regional-impacts-of-sca-and-3-d-secure-20-3ds2--1244971).
- 1090 [32] “SCA for PSD2 could cost merchants more than EUR 100 bln in 2021,” The Paypers,
1091 Sept. 24, 2020. Available at [https://thepayers.com/digital-identity-security-online-
1092 fraud/sca-for-psd2-could-cost-merchants-more-than-eur-100-bln-in-2021--1244803](https://thepayers.com/digital-identity-security-online-fraud/sca-for-psd2-could-cost-merchants-more-than-eur-100-bln-in-2021--1244803).
- 1093 [33] Stephen Ley and Valeria Gallo, Deloitte. “PSD2 standard on secure communication: a
1094 balancing act,” 2017. Available at <https://www2.deloitte.com/ie/en/pages/financial->

- 1095 [services/articles/psd2-standard-on-secure-communication.html](#).
- 1096 [34] European Banking Authority. Final Report: Guidelines on the conditions to benefit from
1097 an exemption from the contingency mechanism under Article 33(6) of Regulation (EU)
1098 2018/389 (RTS of SCA & CSC) (EBA/GL/2018/07). Dec. 4, 2018. Available at
1099 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2250578/4e3b9449-ecf9-4756-8006-cbbe74db6d03/Final%20Report%20on%20Guidelines%20on%20the%20exemption%20o%20the%20fall%20back.pdf>.
- 1103 [35] John Salmon and Jonathan Chertkow, Hogan Lovells. “PSD2: ban on traditional screen
1104 scraping confirmed in final strong customer authentication RTS,” Nov. 29, 2017.
1105 Available at <https://www.engage.hoganlovells.com/knowledgeservices/news/psd2-ban-on-traditional-screen-scraping-confirmed-in-final-strong-customer-authentication-rts>.
- 1107 [36] Patrice Fritsch, EY PFS Solutions. “How to navigate the fallback mechanism exemption
1108 in PSD2?” Mar. 22, 2019. Available at https://www.ey.com/en_lu/payments/psd2--navigating-the-fallback-mechanism-exemption.
- 1110 [37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April
1111 2016 on the protection of natural persons with regard to the processing of personal data
1112 and on the free movement of such data, and repealing Directive 95/46/EC (General Data
1113 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>.
- 1115 [38] Department for Digital Culture, Media and Sport. General Data Protection Regulation
1116 Keeling Schedule. Dec. 18, 2020. Available at
1117 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969514/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted_V4.pdf.
- 1120 [39] European Data Protection Supervisor. Opinion 5/2018: Preliminary Opinion on privacy
1121 by design. May 31, 2018. Available at
1122 https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
- 1124 [40] European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by
1125 Design and by Default, Version 2.0. Oct. 20, 2020. Available at
1126 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
- 1128 [41] Kenneth A. Bamberger, Ran Canetti, Shafi Goldwasser, Rebecca Wexler, and Evan
1129 Joseph Zimmerman. “Verification Dilemmas, Law, and the Promise of Zero-Knowledge
1130 Proofs,” *Berkeley Technology Law Journal*, Vol. 37, No. 1 (forthcoming 2022). Preprint,
1131 May 6, 2021. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781082.
- 1132 [42] Commonwealth of Australia. “What is CDR?” 2021. Available at

- 1133 <https://www.cdr.gov.au/what-is-cdr>.
- 1134 [43] Competition and Consumer (Consumer Data Right) Rules 2020. Compilation No. 3.
1135 Dec. 23, 2020. Available at <https://www.legislation.gov.au/Details/F2021C00076>.
- 1136 [44] Data Standards Body. Consumer Data Standards. 2021. Available at
1137 <https://consumerdatastandardsaustralia.github.io/standards/#introduction>.
- 1138 [45] Australian Competition and Consumer Commission. Compliance Guidance for Data
1139 Holders: Banking sector. April 2021. Available at
1140 <https://www.accc.gov.au/system/files/CDR%20-%20Compliance%20guidance%20for%20data%20holders%20in%20the%20banking%20sector%20-%20April%202021.pdf>.
- 1143 [46] Commonwealth of Australia. “Current Providers,” 2021. Available at
1144 <https://www.cdr.gov.au/find-a-provider>.
- 1145 [47] Australian Competition and Consumer Commission. “Guidance on screen-scraping,”
1146 Mar. 23, 2021. Available at <https://cdr-support.zendesk.com/hc/en-us/articles/900005316646-Guidance-on-screen-scraping>.
- 1148 [48] Eyal Sivan. “Exploring data rights – an interview with James Bligh,” Axway Blog, Jan.
1149 19, 2021. Available at <https://blog.axway.com/digital-strategy/james-bligh>.
- 1150 [49] Australian Competition and Consumer Commission. “Consumer data right (CDR),”
1151 2021. Available at <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>.
- 1152 [50] “About – IndiaStack.” Available at <https://www.indiastack.org/about/>.
- 1153 [51] “About Aadhaar AUTH API – IndiaStack.” Available at
1154 <https://www.indiastack.org/aadhaar/>.
- 1155 [52] “About eKYC API – IndiaStack.” Available at <https://www.indiastack.org/ekyc/>.
- 1156 [53] “About eSign API – IndiaStack.” Available at <https://www.indiastack.org/esign/>.
- 1157 [54] Digital India Corporation. “FAQs.” Available at
1158 <https://www.digilocker.gov.in/about/faq>.
- 1159 [55] Yan Carrière-Swallow, Vikram Haksar, and Manasa Patnam. “India’s Approach to Open
1160 Banking: Some Implications for Financial Inclusion,” IMF Working Paper WP/21/52,
1161 Feb. 26, 2021. Available at
1162 <https://www.imf.org/en/Publications/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Financial-Inclusion-50049>.
- 1164 [56] Vikas Kathuria. “Data Empowerment and Protection Architecture: Concept and
1165 Assessment,” Observer Research Foundation Issue Brief, Issue No. 487, Aug. 12, 2021.

- 1166 Available at <https://www.orfonline.org/research/data-empowerment-and-protection-architecture-concept-and-assessment/>.
1167
- 1168 [57] Vrinda Bhandar and Rahul Narayan. “In Striking Down Section 57, SC Has Curtailed the
1169 Function Creep and Financial Future of Aadhaar,” The Wire, Sept. 28, 2018. Available at
1170 [https://thewire.in/law/in-striking-down-section-57-sc-has-curtailed-the-function-creep-
1171 and-financial-future-of-aadhaar](https://thewire.in/law/in-striking-down-section-57-sc-has-curtailed-the-function-creep-and-financial-future-of-aadhaar).
- 1172 [58] Anand Ramachandran. “The future of Aadhaar and eKYC-based solutions,” The
1173 Economic Times, Mar. 4, 2019. Available at
1174 [https://economictimes.indiatimes.com/small-biz/sme-sector/the-future-of-aadhaar-and-
1175 ekyc-based-solutions/articleshow/68251916.cms](https://economictimes.indiatimes.com/small-biz/sme-sector/the-future-of-aadhaar-and-ekyc-based-solutions/articleshow/68251916.cms).
- 1176 [59] Srinivas Kodali. “How Private Sector Slowly Regained Access to Aadhaar Post SC
1177 Judgment,” The Wire, June 14, 2019. Available at [https://thewire.in/law/aadhaar-rbi-
1178 supreme-court-uidai](https://thewire.in/law/aadhaar-rbi-supreme-court-uidai).
- 1179 [60] Rajeshwar Rao. “Open banking in India,” speech, Apr. 19, 2021. Available at
1180 <https://www.bis.org/review/r210419a.htm>.
- 1181 [61] NITI Aayog. “Data Empowerment and Protection Architecture: Draft for Discussion,”
1182 Aug. 2020. Available at [http://www.niti.gov.in/sites/default/files/2020-09/DEPA-
1183 Book.pdf](http://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf).
- 1184 [62] Eyal Sivan. “The US market-driven approach to Open Banking with Don Cardinal,”
1185 Axway Blog, July 21, 2020. Available at [https://blog.axway.com/amplify-products/api-
1186 management/mr-open-banking-with-don-cardinal](https://blog.axway.com/amplify-products/api-management/mr-open-banking-with-don-cardinal).
- 1187 [63] The Clearing House. “The Clearing House Releases Model Agreement to Help Facilitate
1188 Safe Sharing of Financial Data,” Nov. 12, 2019. Available at
1189 [https://www.theclearinghouse.org/payment-
1190 systems/articles/2019/11/model_agreement_press_release_11-12-19](https://www.theclearinghouse.org/payment-systems/articles/2019/11/model_agreement_press_release_11-12-19) (accessed Aug. 12,
1191 2021).
- 1192 [64] Financial Data Exchange. “Frequently Asked Questions about FDX US.” Available at
1193 [https://financialdataexchange.org/FDX/About/FAQ-
1194 US/FDX/About/FDX_US_FAQ.aspx](https://financialdataexchange.org/FDX/About/FAQ-US/FDX/About/FDX_US_FAQ.aspx).
- 1195 [65] Stan Adams and John B. Morris, Jr., Center for Democracy & Technology. “Open
1196 Banking: Building Trust,” May 26, 2021. Available at [https://cdt.org/wp-
1197 content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf](https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf).
- 1198 [66] Financial Data Exchange. “Financial Data Exchange Launches FDX API 4.2,” Nov. 10,
1199 2020. Available at [https://financialdataexchange.org/FDX/News/Press-
1200 Releases/FDX_Launches_FDX_API_4.2.aspx](https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_FDX_API_4.2.aspx).
- 1201 [67] Financial Data Exchange. OFX Banking Specification, Version 2.3. October 2020.

- 1202 Available at <https://www.ofx.net/downloads.html>.
- 1203 [68] Nacha, "Afinis Interoperability Standards." Available at [https://www.nacha.org/afinis-](https://www.nacha.org/afinis-interoperability-standards)
1204 [interoperability-standards](https://www.nacha.org/afinis-interoperability-standards).
- 1205 [69] U.S. Department of the Treasury. *A Financial System That Creates Economic*
1206 *Opportunities: Nonbank Financials, FinTech, and Innovation*, July 2018. Available at
1207 [https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-](https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-FinTech-and-Innovation.pdf)
1208 [Economic-Opportunities---Nonbank-Financials-FinTech-and-Innovation.pdf](https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-FinTech-and-Innovation.pdf).
- 1209 [70] Consumer Financial Protection Bureau. "Consumer Protection Principles: Consumer-
1210 Authorized Financial Data Sharing and Aggregation," Oct. 18, 2017. Available at
1211 [https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf)
1212 [principles_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).
- 1213 [71] NIST. "Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk
1214 Management, Version 1.0," January 2020.
1215 <https://doi.org/10.6028/NIST.CSWP.01162020>.
- 1216 [72] "ISO/IEC 29100:2011: Information technology — Security techniques — Privacy
1217 framework," 2011.
- 1218 [73] NIST. "Framework for Improving Critical Infrastructure Cybersecurity," April 2018.
1219 <https://doi.org/10.6028/NIST.CSWP.04162018>
- 1220 [74] NIST. "Multi-Party Threshold Cryptography," 2021. Available at
1221 <https://csrc.nist.gov/projects/threshold-cryptography> .

1222 Appendix A—Acronyms

1223	Selected acronyms and abbreviations used in this paper are defined below.	
1224	ANPR	Advance Notice of Proposed Rulemaking
1225	AISP	Account Information Service Provider
1226	API	Application Programming Interface
1227	ASPPS	Account Servicing Payment Service Providers
1228	BNPL	Buy Now Pay Later
1229	CFPB	Consumer Financial Protection Bureau
1230	CIBA	Client Initiated Backchannel Authentication
1231	CM	Consent Manager
1232	CMA	Competition and Markets Authority (U.K.)
1233	DEPA	Data Empowerment and Protection Architecture
1234	e-banking	Electronic Banking
1235	EBA	European Banking Authority (EBA)
1236	FaaS	Finance As A Service
1237	FAPI	Financial-Grade API
1238	FCA	Financial Conduct Authority (U.K.)
1239	FDX	Financial Data Exchange
1240	FS-ISAC	Financial Services Information Sharing and Analysis Center
1241	FI	Financial Institution
1242	KYC	Know Your Customer
1243	MI	Management Information
1244	NACHA	National Automated Clearing House Association
1245	NPCI	National Payments Corporation of India
1246	OB	Open Banking
1247	OBIE	Open Banking Implementation Entity (U.K.)
1248	OFX	Open Financial Exchange
1249	PISP	Payment Initiation Service Provider
1250	PSD2	Revised Payment Services Directive
1251	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

1263 **Appendix B—Glossary**

1264	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.
1265		
1266		
1267		
1268		
1269		
1270	account servicing payment	Banks and other financial institutions
1271	service providers	
1272	banking entity	Any financial institution that conducts business with individuals, such as a retail bank, credit union, or mortgage company.
1273		
1274	central bank	A bank that only interacts directly with other financial institutions (e.g., the U.S. Federal Reserve Bank).
1275		
1276	consent manager	A third-party online intermediary for financial transactions.
1277	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.
1278		
1279		
1280	democratization of data	Making proprietary banking information available to any entity with the owner's permission to access it.
1281		
1282	financial ecosystem	A collection of banking entities and customers conducting financial transactions according to specific rules and governed by a particular set of laws.
1283		
1284		
1285	FinTech	Any financial services company that primarily focuses on internet-based technology to accelerate or enhance conventional services.
1286		
1287	open banking	A special kind of financial ecosystem governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations.
1288		
1289		
1290		