International Journal of Legal Information 51.3, 2023, pp. 197–215. © The Author(s), 2024. Published by International Association of Law Libraries
doi:10.1017/jli.2024.11

Triangular Insight on Open Banking in Indonesia, Singapore, and Australia

Sapto Hermawan*, Zenia Aziz Khoirunisa*, and Kukuh Tejomurti**

Abstract

Open banking is a regulatory framework allowing customers to share their banking data with third-party service providers securely. This concept has gained traction recently, with many countries implementing it to increase competition and innovation in the financial industry. This article will examine how open banking is being implemented in Indonesia, Singapore, and Australia through triangular insight, mainly examining API (Application Programming Interface) standardization, security issues, a regulatory sandbox, customer insights, and user experiences. This article, using normative legal research, demonstrates that open banking is a regulatory framework that is indeed gaining traction in many countries, including Indonesia, Singapore, and Australia. While some challenges and weaknesses are associated with implementing open banking, it can potentially increase competition, innovation, and consumer welfare in the financial industry. Legal research and insights gleaned through triangular insight have been instrumental in developing the legal frameworks for open banking and ensuring that it is implemented securely, transparently, and ethically.

Keywords: Open Banking, Triangular Insight and Analysis, Indonesia, Singapore, Australia

1. Introduction

A "We are Social" report for 2022 indicates that the internet penetration rate in Indonesia reached 73.7% of the total population at the beginning of 2022.[1] As an illustration, the same source reveals that only 73.05 million people were not connected to the internet in Indonesia out of a total of 277.7 million inhabitants. Or to look at it another way, around 26.3% of the population remained offline. The escalation of internet penetration in Indonesia is increasing along with changes in people's lifestyles and the need for social interaction in a digital civilization.[2] One of the impacts of this digital civilization is the presence of technology-based financial services, often known as financial technology (fintech). As of March 2022, there were 102 fintech service providers in Indonesia,[3] and a joint publication of the Institute for Development of Economics and Finance (INDEF) and the Indonesian Fintech Funding Association (AFPI) stated that fintech had significantly contributed Rp60 trillion to the national economy. An added 362,000 workers, directly or indirectly, is considered to have had an impact on reducing poverty by 177,000 people.[4]

* Department of Administrative Law, Faculty of Law, Universitas Sebelas Maret Jalan Ir Sutami 36A Surakarta ID 57126.
** Department of Private Law, Faculty of Law, Universitas Sebelas Maret Surakarta ID.

[1] "Digital 2022: Indonesia," *DataReportal – Global Digital Insights*, https://datareportal.com/reports/digital-2022-indonesia (visited 14 April 2024).

[2] Linda Hantrais and Ashley Thomas Lenihan, "Social dimensions of evidence-based policy in a digital society," 2 *Contemporary Social Science* 16 (2021), at 141.

[3] "Statistik Fintech Lending Periode Maret 2022," https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-Fintech-Lending-Periode-Maret-2022.aspx (visited 14 April 2024).

[4] "Studi Dampak Fintech Peer-To-Peer Lending Terhadap Perekonomian Nasional," *INDEF* (2022), https://web.indef.or.id/research/detail/74 (visited 17 April 2024).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

The statistics for internet usage in 2018, 2019, and 2020 in Australia are vastly different.[5] Despite the global pandemic that has altered how many Australians work and communicate, internet usage in Australia is increasing. More than 86.5% of Australians were online in 2022, with a daily usage time of over 180 minutes (three hours). Australian internet usage is increasing in a business landscape dominated by digital interactions.[6] Meanwhile, at the start of 2022, Singapore's internet penetration rate was 92.0% of the total population. According to Kepios data,[7] the number of internet users in Singapore increased by 43,000 (+0.8%) between 2021 and 2022. For context, these user figures show that 473.6 thousand Singaporeans did not use the internet at the start of 2022, representing 8.0% of the population.[8]

Regarding the internet penetration rate, since July 2020, customers of Australia's largest banks have had the right to share their transaction data with accredited data recipients. This now includes savings, credit cards, loans and mortgages, and transaction accounts. Open banking also applies to other Australian-based, legal, deposit-accepting institutions. Already, sixteen banks, with their sixteen different brands, representing 85% of Australian household savings, are active as data holders. Thirteen data receivers are accredited and active, including fintech, accounting platforms, and benchmarking providers. One of the smaller banks in Australia, as well as the largest, has been accredited to receive customer data from other banks upon request of their customers. Many other big and small entities are undergoing the accreditation process.[9]

In Singapore, 99% of respondents to a 2022 Finastra survey[10] regarded open banking as a "must have" or "important," up from 97% in 2021. The percentage of Singaporean professionals who considered it a "must have" climbed to 64%, a significant increase from 2021 (56%). In 2021, Singapore led other economies with 95% approval that open banking was necessary (global average: 91%) and 47% approval that it was a "must have" (global average: 38%). In 2022, 44% of Singaporeans thought open banking was a must-have, while the global average of 48% suggests that many other markets have followed suit and that the sector is actively studying the products and services that would benefit from ecosystem models. This is not difficult to understand, given that 85% of Singaporean professionals indicated that open finance provides consumers access to a greater variety of financial services. Also, three-quarters (76%) of those professionals concurred that open finance can provide more equitable and fair financial services, and 90% agreed that open finance has benefited the sector and made it more collaborative.

Apart from fintech, another financial service innovation is open banking. The main idea of open banking revolves around banks allowing third-party platforms to access consumer financial data with the consumer's consent and using it to provide additional services or perform transactions on behalf of customers. The OECD sees open banking as an API-based digital platform that allows third parties to access consumer bank data (with the consumer's consent) and is nowadays a fundamental standard of payment with an actual impact of digital disruption.[11] Illustratively, the open banking mechanism can be observed as follows.

At first glimpse, it looks uncomplicated, but open banking is not as simple as the public imagines. Tsai and Peng note that open banking operations require decisive regulations, especially in the broad perspective of comparative legal systems if open banking occurs between countries. Other issues are transaction costs and institutional

[5] "Australia: internet penetration 2022," *Statista*, https://www.statista.com/statistics/680142/australia-internet-penetration/ (visited 17 April 2024); "Australian Internet Statistics 2022," *Red Search*, https://www.redsearch.com.au/resources/australian-internet-statistics/ (visited 24 February 2023).

[6] Liam Ridings, "Australian Internet Statistics 2022 – Essential Facts and Stats" (16 May 2021), *Safari Digital*, https://www.safaridigital.com.au/blog/australian-internet-statistics/ (visited 24 February 2023).

[7] "Quarterly Digital Briefings," *Kepios*, https://kepios.com/briefings (visited 17 April 2024).

[8] "Digital 2022: Singapore" (9 February 2022), *DataReportal – Global Digital Insights*, https://datareportal.com/reports/digital-2022-singapore (visited 17 April 2024).

[9] Australian Banking Association, "Open Banking," https://www.ausbanking.org.au/priorities/open-banking/; Scott Farrell, "The State of Open Banking in Australia in 2021" (2021), https://thepaypers.com/expert-opinion/the-state-of-open-banking-in-australia-in-2021–1253611.

[10] Finastra, Press Release, "Finastra global survey shows appetite for open finance in Singapore against backdrop of constrained investment," Dec. 7, 2022, https://www.finastra.com/sites/default/files/file/2022-12/Press%20release_State-of-the-Nation-Research_Sing_final.pdf; Full survey report available at https://www.finastra.com/sites/default/files/file/2022-12/finastra-financial-services-state-nation-survey-2022.pdf.

[11] OECD, *Digital Disruption in Banking and its Impact on Competition* (2020).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

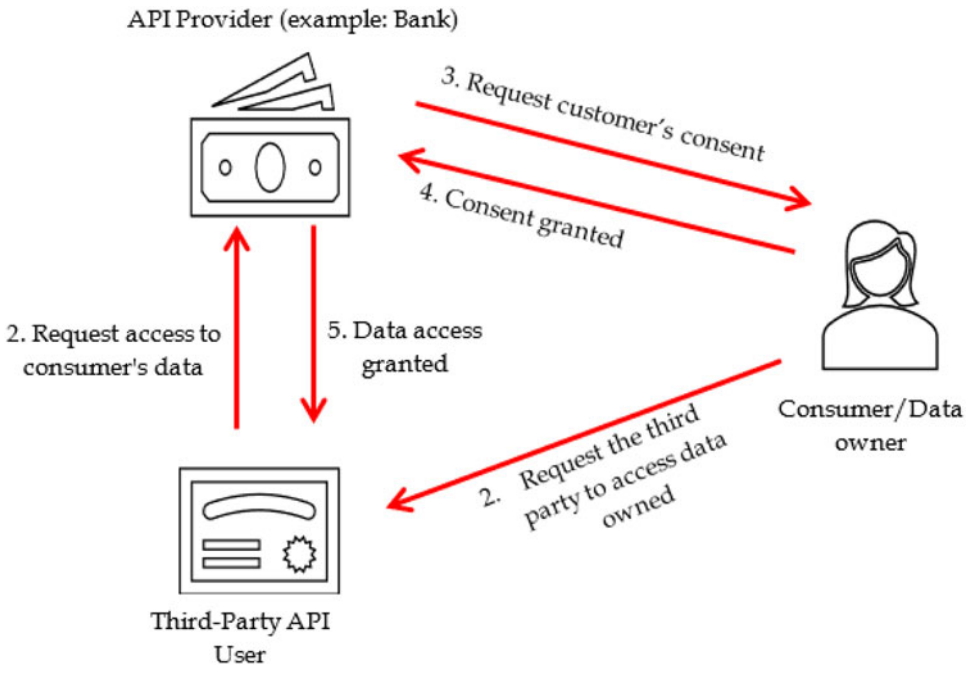


Figure 1. Open Banking Scheme
Source: Sapto Hermawan, Zenia Aziz Khoirunisa, and Kukuh Tejomurti (2023), Open Banking Scheme.

design.[12] Concerning open banking assistance, Babin and Smith encourage governments to adopt a consistent framework that provides the security and protection that consumers need while at the same time providing flexibility for innovation and simplification of banking services using the open banking model.[13]

Several analytic articles have been published previously on this topic, but this article will fill the knowledge gap regarding open banking issues, mainly through triangular insight, where this insight leads to problems for consumers, third parties, and banking as providers of API (Application Programming Interface). This article deliberately compares Indonesia, Singapore, and Australia because these three countries are in relatively close geographic proximity. Second, the growth rate of the use of open banking in the three countries shows a significant increase. This circumstance means that the appreciation and enthusiasm of consumers to change the conventional to revolutionary payment models in these three countries is relatively high.

2. METHODOLOGY

This article uses a mixed legal research method conducted by researching and studying statutes and using comparative and conceptual approaches. The authors also utilized secondary legal materials, such as relevant books, articles, working papers, dissertations, and applicable domestic and international regulations. The technique of collecting legal materials was performed by using library research techniques. The collected data were analyzed using comparative analyses.

3. LITERATURE REVIEW: OPEN BANKING DEFINITION AND FUNDAMENTAL ISSUES

Open banking is a business approach in which data, processes, and business functionalities are available in an ecosystem of banks, customers, and third parties.[14] Implemented through open APIs — software applications that

[12] C-H Tsai and K-J Peng, *Regulating open banking: Comparative analysis of the EU, the UK and Taiwan* (Routledge, 2022).
[13] R Babin and D Smith, "Open banking and regulation: Please advise the government," 2 *Journal of Information Technology Teaching Cases* 12 (2022), at 108.
[14] Theo Lynn, Pierangelo Rosati, and Mark Cummins, "Exploring Open Banking and Banking-as-a-Platform: Opportunities and Risks for Emerging Markets" (Palgrave Macmillan, 2020).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

enable computer systems to communicate and exchange data — customers in open banking can share their bank data with other parties and initiate payments from their bank through third-party apps.[15] This data sharing is conducted through the consent of customers.

The EU's open banking initiative launched from the introduction of the Payment Service Directive 2 (PSD2) that came into force on January 12, 2016, and the EU Member States were required to transpose its provisions into their national laws by January 13, 2018.[16] The PSD2 is the revised version of the original Payment Services Directive (PSD) that the EU introduced in 2007 to create a single payment market within Europe. It set down rules and guidelines for payment services, simplified payment processing across EU countries, advocated innovation, and encouraged competition by opening payments to new entrants.[17] One of the PSD2 aims is to promote innovation in the payments sector, particularly by opening it up to new, non-bank players. This aim is closely related to the formation of the open banking innovation. One example of a successful implementation of open banking is the United Kingdom (UK), where implementing open banking regulations has led to a significant increase in competition and innovation in the financial services sector.[18]

The Open Banking Implementation Entity (OBIE) of the UK was established in 2016 to set the technological and security standards required to enable open banking and to oversee the implementation of the rules.[19] The regulations obligate the nine largest banks in the country to make client data accessible to third-party suppliers via open APIs and with consumer agreement.[20] Since the advent of open banking in the UK in 2018, there has been a significant increase in the number of new fintech companies and other financial service providers joining the market.[21] This scene has resulted in increased competition among providers of financial services, which has boosted consumer options and enhanced services. For example, personal finance management apps that aggregate data from multiple bank accounts have emerged, providing users with a holistic view of their finances. There are additional services that employ machine-learning algorithms to assess a customer's spending habits and advise ways to save money.

Moreover, traditional banks have begun offering open banking services and collaborating with fintech firms to offer new goods and services to their consumers.[22] Generally, the success of open banking in the UK can be credited to OBIE's robust regulatory framework and the collaboration and innovation of banks and fintech companies.[23] The deployment of open banking has produced a more dynamic and customer-focused financial services sector, providing a vivid illustration of the advantages of open banking for consumers and the industry.[24] Learning from the experience of open banking in the UK, this article finds several significant issues that impede the implementation of open banking. This article examines four of these issues, which are also used to analyze Indonesia, Singapore, and Australia.

Some of the problems associated with open banking include the following:

---

[15] Jelena Madir, ed. *Fintech Law and Regulation*, 2nd ed. (Elgar, 2021), at 46.

[16] European Central Bank, "The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security" (2018), https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

[17] Steve Mansfield-Devine, "Open banking: opportunity and danger," 2016 *Computer Fraud & Security* 10 (2016), at 8, https://www.sciencedirect.com/science/article/pii/S136137231630080X.

[18] Open Banking Limited, "Three Years since PSD2 Marked the Start of Open Banking, the UK Has Built a World-leading Ecosystem" (13 January 2021), *News*, https://www.openbanking.org.uk/news/three-years-since-psd2-marked-the-start-of-open-banking-the-uk-has-built-a-world-leading-ecosystem/ (visited 17 April 2024).

[19] Open Banking Limited, *Annual Report 2020* (London: Open Banking Limited, 2020).

[20] NACHA, *API Standardization-Shaping the Financial Services Industry* (2018).

[21] Competition and Markets Authority UK, "Press Release Update on Open Banking" (2021), https://www.gov.uk/government/news/update-on-open-banking.

[22] Emma Leong, "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia and Singapore," 35.3 *Banking & Finance Law Review* (2020), at 1.

[23] Roland Selmer, "Insight: Why Momentum Tells the True UK Open Banking Success Story" (March 2022), *Open Banking Expo*, https://www.openbankingexpo.com/insights/insight-why-momentum-tells-the-true-uk-open-banking-success-story/ (visited 17 April 2024).

[24] Nydia Remolina, "Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-driven World," SMU Centre for AI & Data Governance Research Paper no. 2019/05 (2019), at 36, https://ssrn.com/abstract=3475019.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

A. Security Concerns: Security concerns in open banking refer to the potential risks associated with sharing sensitive financial data with third-party companies. These risks include the following:
   1) Data Breaches. Hackers may target third-party providers or the APIs used to access bank data, leading to the theft of sensitive information. The relationship between open banking data breaches and security concerns is complex and intertwined. Open banking introduces a new level of risk by allowing third-party providers access to sensitive financial information, which can increase the potential for data breaches.[25] At the same time, robust security measures and proper implementation of security protocols can reduce the risk of data breaches and ensure the protection of customer information. Security concerns in open banking include unauthorized access to financial information, hacking, phishing, and malware attacks.[26] To mitigate these risks, banks and third-party providers must adopt strong security measures, such as encryption, multi-factor authentication, and regular security audits. Additionally, customers should protect their information by using strong passwords, monitoring their accounts regularly, and avoiding suspicious emails and links.
   2) Fraud. Fraud is a significant security concern in open banking, as it can result in financial losses and harm to customers.[27] Fraudsters may use phishing, social engineering, and hacking tactics to gain unauthorized access to customers' financial information and steal their money. In open banking systems, fraudsters can target both customers and financial institutions. For example, they may trick customers into revealing their login credentials or steal their identities to open fraudulent bank accounts. They may also target banks and third-party providers by compromising their systems to steal financial information or manipulate transactions.[28]
   3) Phishing Attacks. Phishing attacks in open banking constitute a significant concern for financial institutions and customers. Open banking is a system that allows third-party providers to access banking data and offer services through APIs. Phishing attacks in open banking typically involve using fraudulent emails or websites that appear legitimate to trick customers into providing their login credentials, personal information, or other sensitive data. These attacks can be very sophisticated and challenging to detect, and they often target the weakest link in the security chain — that is, the end user.
   4) Insufficient Security Measures. Insufficient security measures can contribute to security concerns in open banking, leaving customer information and financial transactions vulnerable to fraud and other threats.[29] In the context of open banking, where third-party providers have access to sensitive financial information, it is critical for banks and third-party providers to implement robust security measures to protect against data breaches and other security threats.[30] Examples of insufficient security measures in open banking include weak passwords, a lack of encryption, and poor implementation of multi-factor authentication. If these measures are not in place or implemented effectively, it can increase the risk of unauthorized access to financial information, hacking, and other types of fraud.

B. Lack of Standardization: Different banks have different API implementations, making it difficult for fintech companies to integrate with multiple banks.

   Lack of standardization in open banking refers to the inconsistent implementation of APIs and protocols used by different banks.[31] This deficit can create difficulties for fintech companies that want to offer open banking services, as they have to integrate with each bank's unique API, which can be time-consuming and expensive. The lack of standardization also means that users may experience different levels of quality and reliability when using open banking services, depending on their bank and

[25] Scott Farrell, "Banking on Data: A Comparative Critique of Common-law Open Banking Frameworks," PhD Thesis, The University of New South Wales (2022), at 249, https://doi.org/10.26190/unsworks/24096.

[26] Victor Murinde, Efthymios Rizopoulos, and Markos Zachariadis, "The Impact of the FinTech Revolution on the Future of Banking: Opportunities and Risks," *International Review of Financial Analysis* 81 (2022), at 21.

[27] Hakan Eroglu et al., *PSD2 & Open Banking Security and Fraud Impacts on Banks Are You Ready?* (Accenture, 2016).

[28] KPMG, "Global Banking Fraud Survey The multi-faceted threat of fraud: Are banks up to the challenge?" (May 2019).

[29] See Scott Farrell, n 25, at 11–12.

[30] Faith Reynolds et al., *Consumer Priorities for Open Banking* (2019).

[31] See NACHA, n 20.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

fintech provider. This void can result in a fragmented user experience and lower consumer trust in open banking.

C. Regulation: Open banking is still a relatively new concept that lacks clear and consistent regulation, which can lead to confusion and uncertainty.[32]

Problems with the regulation of open banking refers to the challenges in creating and enforcing clear and consistent regulations for the emerging open banking industry. Some of these issues include the following:

1) Lack of Harmonization. Different countries have different regulations for open banking, leading to a patchwork of rules that can create confusion for fintech companies and banks that operate across borders. The lack of harmonization of open banking regulation refers to the inconsistent regulations across different countries and regions, making it challenging for fintech companies and banks to operate in multiple jurisdictions.[33] This lack of harmonization can lead to the following:
   - Confusion: Different regulations in different countries can create confusion for fintech companies and banks, making it difficult to understand what is expected of them, which potentially leads to legal risks.[34]
   - Barriers to entry: Inconsistent regulations across different countries can create barriers to entry for fintech companies, making it difficult for them to expand into new markets.
   - Fragmented user experience: Different regulations can lead to a fragmented user experience for consumers who use open banking services in different countries.
2) Regulatory Uncertainty. Uncertainty in the regulation of open banking refers to the lack of clear and consistent rules for the emerging open banking industry, making it challenging for fintech companies and banks to understand what is expected of them.[35] This uncertainty can lead to the following:
   - Legal risks: The lack of clear regulations can increase the legal risks for fintech companies and banks that offer open banking services, as they may not fully understand their obligations and responsibilities.
   - Slower adoption: Uncertainty in regulation can make it difficult for fintech companies and banks to confidently invest in and adopt open banking technologies and services, slowing the development and adoption of the industry.
   - Lack of consumer trust: Uncertainty in regulation can reduce consumer trust in open banking, as consumers may be concerned about the security of their financial data and the financial system's stability.
   - Inconsistent practices: The lack of clear regulations can also result in inconsistent practices among different providers, creating confusion for customers and hindering the development of a robust open banking ecosystem.
3) Compliance Costs. Compliance costs in open banking refers to the expenses that financial institutions and fintech companies incur to comply with regulations related to open banking. Compliance costs can be high and a barrier to entry for smaller players in the market. Some of the factors that contribute to compliance costs in open banking are the following:
   - Complex regulations: Open banking regulations can be complex and challenging to understand. This issue can require significant time and resources to interpret and implement, leading to increased compliance costs.
   - Multiple regulations: In some cases, financial institutions and fintech companies may be subject to multiple regulations related to open banking, depending on the jurisdictions in which they operate. These issues can increase compliance costs and make complying with all relevant regulations more complex.

[32] Faith Reynolds, *Open Banking: A Consumer Perspective* (2017).

[33] Marius Galdikas, "Does Open Banking Live Up to Its Claims? Key Aspects that Hinder Smooth Transactions" (February 2022), https://thepaypers.com/thought-leader-insights/does-open-banking-live-up-to-its-claims-key-aspects-that-hinder-smooth-transactions–1254627 (visited 17 April 2024).

[34] See Scott Farrell, n 25, at 24.

[35] OECD, *Data Portability in Open Banking Privacy and Other Cross-cutting Issues* (2023), https://www.oecd.org/digital/data-portability-in-open-banking-6c872949-en.htm.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

- Compliance monitoring: Financial institutions and fintech companies may need to invest in compliance monitoring systems to meet all regulatory requirements. These systems can be expensive and time-consuming to implement, particularly for smaller players in the market.
- Penalties for non-compliance: Financial institutions and fintech companies may face significant penalties for non-compliance with open banking regulations, which can create an additional financial burden and cause reputational damage.

4) Differing Standards. Differing standards in open banking refers to the lack of consistent technical standards and protocols for sharing data between financial institutions and fintech companies in different regions and countries.[36] These differences can create difficulties for financial institutions and fintech companies in developing and implementing open banking systems that can be easily integrated with other systems.

D. Customer Concerns and User Experience: Open banking involves sharing sensitive financial data, which can make customers feel uncomfortable or anxious about the security of their data. This situation can limit the adoption of open banking initiatives and slow the growth of the open banking industry. User experience is another problem associated with implementing open banking.[37] While open banking has the potential to provide customers with new and innovative financial services, the complexity of data-sharing systems and protocols can create a confusing and frustrating experience for customers. For example, customers may be required to navigate multiple authentication processes and user interfaces when accessing financial services from different providers, which can be time-consuming and confusing. Customers may also be required to manually enter their financial data into different systems, which can be tedious and error-prone. This article assumes that several factors cause customer concerns and negative user experiences as follows:

- Customer awareness. Customer awareness is a significant challenge in open banking regulation, as many consumers are unaware of what open banking is and how it can benefit them. This lack of awareness can lead to the slow adoption of open banking services and reduce the potential benefits of the technology.
- Lack of education. Consumers may be unaware of open banking services because they have not been adequately educated about the technology and its potential benefits.
- Complexity of system architecture. Accessing and using open banking services can be complex, and consumers may hesitate to use the technology because they do not fully understand it.[38]
- Lack of trust. Consumers may hesitate to use open banking services because of security concerns or a lack of trust in the technology.[39] The consumer does not ensure that regulations are in place to protect their financial data, and the industry has no transparency or mechanisms to build trust with consumers.

4. RESULT AND DISCUSSION

4.1. Factsheet on Open Banking in Indonesia, Singapore, and Australia

Open banking represents a significant transformation in the financial services industry and is the first step towards a big data economy in many other industries (telecom, energy, utilities, etc.).[40] Open banking gives

[36] Abdulaziz Almehrej, Leo Freitas, and Paolo Modesti, *Account and Transaction Protocol of the Open Banking Standard* (Springer, 2020).

[37] See Nydia Remolina, n 24, at 32.

[38] Monetary Authority of Singapore and The Association of Banks in Singapore, *ABS-MAS Financial World | Finance-as-a-Service: API Playbook* (2016), at 8.

[39] Chengzu Dong et al., *BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity* (Springer Science and Business Media Deutschland GmbH, 2020).

[40] Markos Zachariadis and Pinar Ozcan, "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking," *Swift Institute Working Paper* no. 2016-001 (2017), at 2.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

consumers greater control over their data and will drive faster and more valuable innovations for consumers.[41] This article provides a triangular insight into three countries implementing open banking—Indonesia, Singapore, and Australia. The reference architecture presented in this article will help readers understand the development of open banking solutions by considering fundamental aspects, including API technical standards, security standards, regulatory adequacy, and consumer protection and satisfaction. The table below explains the juridical perspective of implementing open banking in Indonesia, Singapore, and Australia.

Indonesia has launched an open banking policy as a country with great digital economic potential. Open banking in Indonesia is based on the 2025 Indonesian Payment System Blueprint (BSPI 2025) issued by Bank Indonesia (BI).[42] BSPI 2025 is BI's payment system policy for navigating the role of the payment system industry in the digital economy and finance era;[43] the blueprint contains five payment system visions, one of which is open banking. As stated in BSPI 2025, open banking aims to encourage digital transformation in the banking sector and build links between banks and fintech.

To assist Indonesia's open banking development in a structured and systematic manner, BI created the Open API Framework. BI also constructed the National Payment Open API Standard (Standar Nasional Open API Pembayaran, SNAP) as the derivative of the framework.[44] Together with the Indonesian Payment System Association (ASPI), the National Working Group was established to prepare SNAP. Before the working group was formed, BI issued a Consultative Paper on Open API Payment Standards in March 2020.[45] The implementation of open banking in Indonesia has been adopted by several banks included on BI's open banking API list. The banks have various goals, such as accelerating fintech innovation, developing virtual account and direct debit services for transactions, accessing product information, and targeting the market for fintech and e-commerce players. The banks also actively collaborate with fintech startups to build API services and products and facilitate digital banking transactions at home and abroad.[46]

As an early adopter of open banking in the Asia-Pacific region, Singapore was touted as a leader of open banking and API within the region in the Open Banking APAC report compiled by the Emerging Payments Association Asia (EPAA), which was released in February 2020.[47] This report cannot be separated from the role of the Monetary Authority of Singapore (MAS) as the developer of open banking in Singapore. In November 2018, MAS introduced the API Exchange (APIX), a collaboration platform, as the foundation for the growth of open banking in Singapore.[48] APIX aims to support financial innovation and inclusion in ASEAN and worldwide so that it becomes the first open-architecture platform on an international scale.[49] Through APIX, financial institutions and fintech firms can connect quickly and collaborate on design experiences via APIs.

In collaboration with the Association of Banks in Singapore (ABS), MAS published the "Financial World: Finance-As-A-Service API Playbook" in 2016 as a comprehensive guideline for financial institutions and fintech

[41] Ministry of Foreign Affairs of the Netherlands, *The Role of Consumer Consent in Open Banking* (2021).

[42] Paripurna P Sugarda and Muhammad Rifky Wicaksono, "Enhancing the Competitiveness of Indonesia's Financial Services Sector in the Digital Era Through Open Banking: Lessons Learned from the UK's Experience," 1 *Journal of Central Banking Law and Institutions* 2 (2023), at 161.

[43] Bank Indonesia, 'Blueprint Sistem Pembayaran Indonesia 2025' (2019), www.bi.go.id.

[44] Camila Amalia et al., "Legal Issues of Personal Data Protection and Consumer Protection in the Open API Payments," 2 *Journal of Central Banking Law and Institutions* 1 (2022), at 329.

[45] Bank Indonesia, "Bank Indonesia Launches National Open API Payment Standard and Sandbox Trials of QRIS and Thai QR Payment Interconnectivity" (August 2021), https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2321121.aspx (visited 17 April 2024).

[46] Brick, "Mengenal Open Banking API di Perbankan Indonesia dalam Perkembangan Layanan Finansial" (October 2021), https://www.onebrick.io/id/about/blog/mengenal-open-banking-api-di-perbankan-indonesia-dalam-perkembangan-layanan-finan/ (visited 22 July 2022).

[47] See Fintech Singapore, "What Does Singapore's Open Banking Landscape Look Like in 2021?" (30 June 2021), *Fintech Singapore*, https://fintechnews.sg/52211/openbanking/what-does-singapores-open-banking-landscape-look-like-in-2021/ (visited 17 April 2024).

[48] Monetary Authority of Singapore, "API Exchange (APIX)" (2021), https://www.mas.gov.sg/development/fintech/api-exchange (visited 26 July 2022).

[49] Singapore Government Developer Portal, "API Exchange (APEX) - A Centralised Data Sharing Platform for the Public Sector" (October 2022), https://www.developer.tech.gov.sg/products/categories/data-and-apis/apex/overview.html (visited 17 April 2024).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

TABLE 1:
Regulatory Sandbox Open Banking

Differentiating Factors	Indonesia	Singapore	Australia
Initiative	Indonesian Payment System Blueprint (2025)	Finance as a Service: API Playbook (2016)	Consumer Data Rights Legislation (2010)
Authority	Bank Indonesia (BI)	Monetary Authority of Singapore (MAS)	Australian Competition and Consumer Commission (ACCC)
Scope of Policy	– Transfer and Payment – Product Subscription – Account information	– Payment Status – Transaction Initiation – Account Information – Product Information	– Consumer-data – Transaction-data – Product information

Sources: Bank Indonesia, 2021, Bank Indonesia Launches National Open API Payment Standard and Sandbox Trials of QRIS and Thai QR Payment Interconnectivity; Bank Indonesia, 2019, Blueprint Sistem Pembayaran Indonesia 2025.

companies to adopt and develop API systems for their organizations. To consolidate the financial data from banks and government agencies in a single place, MAS also launched the Singapore Financial Data Exchange (SGFinDex) on December 7, 2020, in collaboration with ABS and seven participating banks.[50] This initiative aims to facilitate data portability with a secure API framework. Singaporeans use Singapore Personal Access (SingPass) as a single sign-on service to transact with multiple government agencies online.[51] Consumers can share their information with financial institutions based on their consent. Therefore, SingPass became the world's first public digital infrastructure using national identity, that is centrally managed through an online system based on consent.[52]

MAS also operates the Financial Industry API Register, which serves as the initial landing site for open APIs available in the Singapore financial industry. The register is updated continuously as financial institutions make their open APIs available. The open APIs are classified into the following main functional categories:[53]

- Product APIs (e.g., to provide information on financial product details and exchange rates)
- Sales & Marketing APIs (e.g., to handle product sign-ups, sales/cross-sales, and lead generation)
- Servicing APIs (e.g., to manage customer profile/account details and customer queries/feedback)
- Transaction APIs (e.g., to support customer instructions for payments, fund transfers, settlements, clearing, trade confirmations, and trading)

Each functional category is further classified as either transactional (i.e., sensitive client data, user/partner authentication required) or informational (i.e., non-sensitive data, no/minimal authentication required). In implementing the API framework, Singapore bases its implementation on the following principles: openness, usability, interoperability, reuse, independence, stability, extensibility, loosely coupled, and transparency.

Meanwhile, in Australia, the first phase of open banking began with the introduction of the Consumer Data Right (CDR) legislation on July 1, 2020.[54] Banking was the first sector in which this right was applied.[55] Open banking allows Australians to share their banking data with third parties accredited by the Australian

[50] Monetary Authority of Singapore, "Digital Infrastructure to Enable More Effective Financial Planning by Singaporeans" (7 December 2020), https://www.mas.gov.sg/news/media-releases/2020/digital-infrastructure-to-enable-more-effective-financial-planning-by-singaporeans (visited 17 April 2024).

[51] Government Technology Agency Singapore, "SingPass - Singapore's National Digital Identity" (Sep, 18, 2024), https://www.singpass.gov.sg/main/trusted-identity.

[52] Gina Clarke, "Singapore Launches World's First Public-Private Partnership to Create A New Digital Infrastructure" (December 2020), *The Fintech Times*, https://thefintechtimes.com/singapore-launches-worlds-first-public-private-partnership-to-create-a-new-digital-infrastructure/ (visited 17 April 2024).

[53] Monetary Authority of Singapore (MAS), "Financial Industry API Register," https://www.mas.gov.sg/development/fintech/financial-industry-api-register (visited 17 April 2024).

[54] See Scott Farrell, n 25, at 25.

[55] Rachel Gauci, "Is Europe a good Example of Open Banking?," in *The PayTech Book*, eds. S. Chisti et al. (Wiley, 2020), https://doi.org/10.1002/9781119551973.ch25.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

Competition and Consumer Commission (ACCC). Australians can also permit accredited third parties to access mortgages, personal loans, and joint bank account data. This allows bank customers to search for better deals on banking products or keep track of their banking in one place.[56]

The development of open banking in Australia is divided into different phases. In 'Phase I,' consumer data, such as savings, debit, or credit card accounts, had to be shared by non-major ADIs (Authorized Deposit-taking Institutions) from July 1, 2020.[57] From November 1, 2020, they had to start sharing 'Phase 2' data, including residential home loans, investment property loans, and personal loans. Finally, 'Phase 3' was the deadline for the other banks to provide accounts and transactions such as investment loans, asset finance, and retirement savings accounts by February 2022.[58] The four major Australian banks have shared consumer data for all phases since the first.[59]

The open banking system in Australia already involves sixteen banks, with sixteen different brands, representing 85% of Australia's household deposits.[60] Thirteen data recipients, including fintech, accounting platforms, and comparison providers, have been active and accredited. One of Australia's smaller banks, as well as the largest, is already accredited to receive customers' data from other banks at their customers' requests. Both large and small entities are cycling through the ongoing accreditation process. The accreditation also allows customer-driven data sharing in other sectors, such as energy and telecommunications.[61] A study conducted by Australian fintech company Frollo and lending technology provider NextGen.Net revealed much excitement about open banking within Australia's financial services industry, with 71% of respondents, including banks, brokers, and fintech companies, stating that they intended to use CDR data.[62] Among the key challenges that respondents cited for making the CDR regime a success were complexity/clarity of the rules (54.2%), customer education (50%), compliance (45.8%), and cost (29.2%).

4.2. Triangular Analysis of Open Banking in Indonesia, Singapore, and Australia

4.2.1 Indonesia

In Indonesia, several third-party providers have emerged to offer open banking services, including fintech companies, payment providers, and other financial technology companies.[63] These third-party providers offer various services, ranging from payment processing and remittances, to loans and financial planning. The use of open banking in Indonesia is still in its early stages, and the regulatory framework for open banking is still being developed.[64] However, the growth of open banking in Indonesia can bring significant benefits to consumers and the broader financial sector, including increased competition, improved financial inclusion, and enhanced financial services.[65] The following sections investigate the implementation of open banking in Indonesia based on indicators of security concerns, a regulatory sandbox, application standardization, user experience, and customer satisfaction.

Security concerns are a significant challenge for developing open banking in Indonesia. Open banking requires sharing sensitive financial data, which can increase the risk of data breaches and fraud. Based on the literature review, open banking in Indonesia still faces some challenging issues:

- Data Breaches: The potential for data breaches and unauthorized access to financial data is a significant concern in open banking. Data breaches can include hacking, phishing, and other types of cyberattacks that can result in the theft of sensitive financial information.

[56] See Australian Banking Association, n 9; AM Dahdal and B Zeiler, "Open Banking and Open Data: Global Context, Innovation, and Consumer Protection," 7 *Banking Law Journal* 138 (2021), at 385.

[57] Australian Banking Association, "Open Banking Timeline," https://www.ausbanking.org.au/insight/open-banking-timeline/ (visited 17 April 2024).

[58] Australian Goverment, *Phasing*, Consumer Data Right (Australia, 2020).

[59] See Australian Banking Association, n 9.

[60] See Scott Farrell, n 25.

[61] Ibid., at 79.

[62] Frollo and Nextgen.Net, "The State of Open Banking Report 2020" (2020), https://frollo.com.au/open-banking/state-of-open-banking-report-2020/ (visited 17 August 2022).

[63] See Bank Indonesia, n 43, at 27.

[64] Otoritas Jasa Keuangan Republik Indonesia, *Digital Finance Innovation Road Map and Action Plan 2020–2024* (2020).

[65] See Bank Indonesia, n 43, at 28.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

- Fraud: Fraud is also a significant concern in open banking, particularly in the context of third-party providers. Financial institutions and regulatory authorities must work together to ensure appropriate measures are in place to prevent and detect fraud.
- Lack of Regulation: The lack of a comprehensive regulatory framework for open banking in Indonesia can also contribute to security concerns. This regulation can include a lack of clear data protection, privacy standards, and oversight and enforcement mechanisms.
- Technical Issues: Technical issues, such as software vulnerabilities, can also contribute to security concerns in open banking. Financial institutions and third-party providers must invest in robust security systems and procedures to minimize the risk of technical issues that could compromise the security of financial information.

Furthermore, the lack of standardization is one of the challenges facing the development of open banking in Indonesia.[66] Standardization refers to developing consistent standards and protocols for data sharing and security in open banking.[67] Standardization is critical to ensure that financial data can be easily and securely shared between financial institutions and third-party providers and to build trust in the security of these services. The lack of standardization in open banking in Indonesia can lead to several challenges, including the following:

- Inconsistent Data Sharing: The lack of standardization can result in inconsistent data-sharing practices between financial institutions and third-party providers, making it difficult for customers to compare and use different open banking services.
- Incompatible Systems: Financial institutions and third-party providers may develop incompatible systems without consistent standards, making it difficult to share data between them, potentially leading to security vulnerabilities.
- Fragmented Market: The lack of standardization can also result in a fragmented market, with different financial institutions and third-party providers offering inconsistent customer services and experiences.
- Slow Adoption: The lack of standardization can also slow the adoption of open banking services, as customers may be hesitant to use these services if they are uncertain about the security of their financial data.

The regulatory sandbox is a regulatory framework under which fintech companies can test their products on real-world consumers in a controlled, demarcated market space while benefitting from certain temporary exemptions from full compliance with the relevant regulatory regimes, albeit under the supervision of a regulator.[68] National regulators often struggle to enforce existing regulations or implement new ones in the evolving business environment. Many fintech companies and financial institutions are uncertain about how they can implement innovative technologies in a regulatory-compliant manner.[69] This condition also applies to open banking arrangements in Indonesia. Due to this absence of a regulatory sandbox, open APIs applied in Indonesia tend to be varied and not standardized regarding cooperation contracts, API technicalities, and security.[70] Open API is also implemented only in a limited scope with specific contract schemes, generally in bilateral contracts through open-partner APIs.

The regulatory framework for open banking in Indonesia has several weaknesses that can impact the growth and development of these services. Some of the key challenges are the following:

- Lack of a Clear Regulation: The regulatory framework for open banking in Indonesia is still in the early stages of development, and there is a lack of clear and comprehensive regulation. This problem can create uncertainty for financial institutions and third-party providers, making investing in and developing open banking services difficult.

  At the time of this writing, there was no regulation regarding the practice of open banking in Indonesia. The implementation of open banking in Indonesia is only based on the open API framework created by Bank Indonesia. This framework is a kind of policy and is not legally binding on the parties. Here, there is a legal vacuum that can result in legal uncertainty. Legal certainty can be defined in six ways. First, legal certainty

[66] Billiam Billiam, Lastuti Abubakar, and Tri Handayani, "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking," 1 *Padjadjaran Jurnal Ilmu Hukum* 9 (2022), at 72.

[67] See Scott Farrell, n 25, at 113.

[68] See Jelena Madir, ed., n 15, at 341.

[69] Hilary J Allen et al., "Regulatory Sandboxes," *George Washington Law Review* 87 (2019), at 606.

[70] See Bank Indonesia, n 43, at 33.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

can be understood as a certainty of law in the sense that for the law to be considered "reliable," it must have objective qualities such as clarity and determinacy.[71] Legal uncertainty under this definition will lead to unclarity and indeterminacy, making the law "unreliable." The unclarity and indeterminacy of legal norms regarding open banking in Indonesia create a uniform standard in its implementation. Second, legal certainty can be understood as certainty through law. Legal certainty within this meaning represents guaranteeing certainty (i.e., an "assurance" of rights and obligations).[72] Meanwhile, legal uncertainty may hinder the fulfillment of other rights guarantees. The parties involved in implementing open banking in Indonesia have no assurance of rights and obligations to carry out open banking operations in Indonesia, which should be obtained through the law.

Third, legal certainty can be understood as certainty before the law. Law, in this definition, does not play a role as an instrument to guarantee certainty but rather as an object that causes it.[73] Indonesia still has 91 million people who do not have access to financial institutions out of the total adult population of 181 million residents.[74] Since the regulation regarding open banking is not formed yet, the exclusivity of access to financial institutions will remain. The open banking regulation should be a norm that causes those "unbanked" populations to have equal access to open banking. Therefore, there is no certainty before the law in this case. Fourth, legal certainty can be understood as a certainty of the individual under the individual protection of the law.[75] Individual norms become the main focus of assuring certainty through the law and certainty of rights. In open banking, consumer data protection is a fundamental aspect to highlight. However, in Indonesia, the absence of an open banking regulation creates unclear provisions regarding what types of data will be protected, whether general, personal, or specific. As a result, personal protection through the law becomes blurry. Fifth, legal certainty can be used not to refer "to the law," "to rights," or "to the right," but instead "as a right." This meaning only shows that the legal certainty principle can function as a subjective right from the concrete and subjective point of view.[76]

Legal uncertainty can be a significant factor in attempting to fulfill the right to legal certainty. The parties and the consumers involved should have the right to legal certainty in Indonesia's open banking system. Sixth, legal certainty may denote a state of certainty not through the law but through a specific right. In this definite sense, one can say that a citizen's right to be notified of the inclusion of new evidence in a suit, for instance, increases this citizen's understanding of the opposite party's position.[77] Open banking involves several parties in its implementation: banks, customers, and third parties. When there is a dispute (i.e., defaulting), overlapping obligations have the potential to occur. Regulations should determine the extent of each party's liability.

- Data Protection and Privacy: Data protection and privacy regulation are essential for open banking. In Indonesia, there is a lack of clear regulations and standards to ensure the security and privacy of financial data shared between financial institutions and third-party providers.
- Technical Interoperability: The lack of clear technical standards and interoperability requirements can also impact the development of open banking in Indonesia. The absence of clear technical standards can make it difficult for financial institutions and third-party providers to exchange data effectively, impacting the usability and reliability of open banking services.
- Lack of a norm for valuing consumer awareness: Another challenge is the lack of awareness about open banking services. Customers may hesitate to adopt these services without clear and concise information about their workings and potential risks and benefits.

Unfortunately, this article cannot point to specific empirical evidence on the user experience of open banking in Indonesia. However, studies and surveys of open banking customers in Indonesia could provide valuable insight into the user experience of these services. These studies could explore topics such as those listed below:

- Adoption Rates: Studies could look at the adoption rate of open banking services among Indonesian consumers and compare this to adoption rates in other countries.

---

[71] Humberto Ávila, *Certainty in Law* (Springer International Publishing, 2016), at 72.
[72] Ibid., at 73.
[73] Ibid., at 75.
[74] Asian Banker, "Digitalisation Paving the Way to Financial Inclusion," *Finance Indonesia 2022*, https://theasianbanker.com/finance-indonesia-2022/ (visited 17 April 2024).
[75] See Humberto Ávila, n 71, at 75.
[76] Ibid., at 75.
[77] Ibid., at 76.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

- User Satisfaction: Surveys could explore the level of satisfaction among open banking customers in Indonesia, including factors such as the ease of use of these services, the reliability of the services, and the level of customer support available.
- User Behaviors: Studies could examine the behaviors and attitudes of open banking users in Indonesia, including their motivations for using these services, their perceived benefits and risks, and their levels of trust in these services.
- Market Trends: Surveys and studies could also look at market trends and changes in the open banking sector in Indonesia, including the growth in the number of new providers and the emergence of new services and technologies.

This kind of data could provide valuable insight into the user experience of open banking in Indonesia and inform the development of these services. However, the availability and accessibility of these studies may be limited by factors such as (1) the open banking development stage in Indonesia, (2) the size of the customer base, and (3) the availability of research funding and resources. Moreover, the authors of this article had no access to up-to-date information on adopting open banking services among Indonesian consumers and no up-to-date information on Indonesia's satisfaction levels of open banking customers. However, customer satisfaction is a vital indicator of the success and viability of open banking services.[78]

In summary, Indonesian consumers do not want their private information leaked without permission. These leaks could result in personal information misconduct.[79] Open banking in Indonesia indeed has this kind of grey area of data security—for example, how much consumer data can be shared with various parties, which types of data, and whether it can be done all the time or only when the transaction occurs. The user authentification issue is also at a point where there is a possibility that a user of a Third Party Protocol (TPP) application can obtain authorized access to a bank account that is perhaps under the control of someone else.

Moreover, when third parties get involved, and the number of them keeps rising, there is no guarantee to ensure that the same security standards are being followed. Open banking will be making TPPs part of the security perimeter of financial institutions' IT infrastructures, posing systemic cyber risks across organizations and third parties. This breaching potential is related to the absence of regulations that comprehensively regulate data security in open banking in Indonesia. When things go wrong, the banks will likely end up with the lion's share of the liability without sufficient control over the whole process to fully control the risks.[80]

4.2.2 Singapore

Open banking in Singapore has been growing in recent years, and as with any new financial technology, security concerns need to be addressed. Some of the critical security concerns related to open banking in Singapore include the following:

- Data Breaches: There is a risk that sensitive financial information, such as bank account numbers and balances, could be stolen or misused in the event of a data breach. This risk is increased when financial information is shared between multiple parties.
- Phishing and Fraud: Open banking makes it easier for criminals to impersonate legitimate financial institutions and trick consumers into revealing their financial information. Phishing scams, in particular, have become a common method of attack in the open banking ecosystem.
- Lack of Security Standards: There is currently a lack of standardization in the open banking ecosystem in Singapore, which makes it difficult for consumers to understand the security measures in place and compare the security of different providers.[81] This security standard can increase the risk of security incidents.
- Third-party Risk: When financial information is shared with third-party providers, there is a risk that the provider could be hacked or the security of the information compromised. This risk is increased when third-party providers have access to sensitive financial information over an extended period.

However, the empirical evidence suggests that there is still room for improvement in terms of security in the open banking ecosystem in Singapore. For example, a survey conducted by Accenture in 2020 found that 49% of

[78] Christian Ball, "Why Data Has Become Banks Most Important Commodity" (2017), *Global Banking & Finance Review*, https://www.globalbankingandfinance.com/why-data-has-become-banks-most-important-commodity/ (visited 17 April 2024).
[79] See Chengzu Dong et al., n 39.
[80] See Mansfield-Devine, n 17.
[81] See Monetary Authority of Singapore and The Association of Banks in Singapore, n 38, at 8.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

consumers in Singapore were generally distrustful of digital banking services.[82] This evidence suggests that there is a need for further work to be done to improve consumer trust in open banking and to address security concerns. In sum, while open banking has the potential to bring many benefits to consumers and financial institutions, it is crucial to be aware of the security risks and to take steps to mitigate these risks. Ongoing monitoring and improvement will be necessary to ensure the security of sensitive financial information in the open banking ecosystem in Singapore.

Furthermore, at the time of this writing, there was no specific empirical data available on the lack of standardization in Singapore's open banking system. Open banking is a relatively new concept, and various organizations and regulatory bodies are working on development and standardization. It is also possible that data on the lack of standardization may not be publicly available or widely published. However, this article's authors believe that the lack of standardization in the open banking ecosystem is a common concern across many countries, including Singapore. A lack of standardization can make it difficult for consumers to understand the security measures and compare the security of different providers. It can also make it more difficult for financial institutions and third-party providers to understand their responsibilities and obligations under the open banking framework. In sum, the lack of standardization in open banking is a common concern, and regulators and financial institutions must address this issue and ensure that the open banking ecosystem is secure and trustworthy for consumers.

Open banking regulation in Singapore is still a relatively new concept, and as with any new regulation, some weaknesses need to be addressed. Some of the weaknesses of open banking regulation in Singapore include the following:

- Lack of Consumer Awareness: Many consumers in Singapore are still unaware of open banking and how it works. This problem can lead to a lack of trust in the system and low adoption rates. Traditional financial institutions may resist open banking as it could disrupt their traditional business models and increase competition. This could slow the adoption of open banking and limit its potential benefits to consumers.
- Data Privacy Concerns: With open banking, financial institutions must share customer data with third-party providers. This has raised concerns about protecting sensitive information and the potential for data breaches.
- Regulation Gaps: There are still regulatory gaps in open banking, which can lead to a lack of consistency in how different financial institutions implement the regulation.
- Lack of a Norm for API Standardization: There is a lack of standardization in how different financial institutions implement open banking, which can lead to inconsistencies and difficulties for consumers who want to use the services of multiple providers.
- Lack of a Norm for Cybersecurity Risks: Open banking increases the risk of cyberattacks and data breaches as more sensitive information is shared between financial institutions and third-party providers.
- Compliance Costs: Implementing open banking can be costly for financial institutions, particularly smaller ones, and they may be required to make significant investments in technology and infrastructure to meet regulatory requirements.

This article's authors had no access to the latest empirical evidence on the user experience of open banking in Singapore. However, the authors believe that user experience with open banking generally varies depending on factors such as the security and reliability of the third-party providers, the ease of use of the open banking platform, and the level of customer support provided by financial institutions. It is important to note that the success of open banking depends on the ability of financial institutions and third-party providers to address customers' security concerns and provide a user-friendly and reliable experience. This reliable architecture can include clear and concise explanations of how open banking works, easy access to financial data, and robust security measures to protect sensitive information.

4.2.3 Australia

Like Indonesia and Singapore, open banking in Australia has various security concerns, just like any other financial system dealing with sensitive financial information. Some of the security concerns include the following:

- Data Breaches: Open banking requires sharing sensitive financial information, potentially leading to data breaches if the information is not adequately secured.
- Phishing Scams: Phishing scams are a common threat in the financial industry, and open banking is no exception. Scammers may trick consumers into giving away their financial information, which could lead to financial losses.

[82] Accenture, "Making Digital Banking More Human," 2020 Accenture Global Banking Consumer Survey (2020), at p. 11, https://www.retail-fcl.com/wp-content/uploads/2021/06/Accenture-Banking-Consumer-Study-2020.pdf.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

- Unauthorized Access: If third-party providers do not have proper security measures, they may be vulnerable to unauthorized access, resulting in the loss or misuse of sensitive financial information.
- Malicious Software: Malicious software, such as malware, can infect computers and steal financial information. Consumers need to keep their devices and software up-to-date to reduce the risk of infection.

It is crucial for Australian consumers to be aware of these security concerns and to take steps to protect their financial information when using open banking services. This awareness includes being cautious of phishing scams, using strong passwords, and only using trusted third-party providers. Additionally, consumers should regularly monitor their financial accounts and immediately report suspicious activity to their banks. Limited empirical data is available on the security concerns of open banking in Australia. However, as open banking continues to gain popularity, there have been reports of security incidents and data breaches involving financial information shared through open banking APIs.

For example, in 2019, the Australian Securities and Investments Commission (ASIC) reported that several financial institutions had suffered data breaches due to the theft of API keys to access sensitive financial information. In another instance, a security researcher found an open banking API vulnerability that could have allowed an attacker to access sensitive financial information, such as bank account numbers and transaction histories. These incidents demonstrate the need for ongoing vigilance and attention to security in the open banking ecosystem. Financial institutions and third-party providers must ensure robust security measures to protect sensitive financial information, and consumers must be aware of the potential risks and take steps to protect themselves.

Furthermore, the lack of standardization in open banking can significantly impact its security. Without a standard set of rules and protocols for accessing and sharing financial information, the risk of security incidents and data breaches increases. Empirical data supports the idea that a lack of standardization can lead to security issues in open banking. For example, a study by the Australian Prudential Regulation Authority (APRA) found that financial institutions using different protocols and security standards for open banking had a higher risk of security incidents than those using a standardized approach.[83] Additionally, the Australian Competition and Consumer Commission (ACCC) has reported that inconsistencies in implementing open banking by different financial institutions can make it difficult for consumers to understand how their financial information is being used and protected.[84] These inconsistencies can lead to confusion and mistrust and make it harder for consumers to make informed decisions about their financial information. In sum, the lack of standardization in open banking in Australia can have profound implications for security and consumer trust. Financial institutions and regulatory authorities must work together to develop a standardized approach to open banking that prioritizes security and consumer protection.

Limited empirical data on the relationship between a lack of standardization and security concerns in Australian open banking is available. However, a lack of standardization in the open banking ecosystem can create challenges for financial institutions and consumers, including security risks. For example, with the lack of a standardized API, financial institutions may have to develop their APIs, which could lead to inconsistencies in security measures and increase the risk of data breaches. Furthermore, third-party providers might use different methods to access financial information, making it more difficult for consumers to understand the security measures in place and compare the security of different providers.

On the other hand, standardization could help improve the security of the open banking ecosystem by providing a consistent set of guidelines for financial institutions and third-party providers to follow. This standardization could increase confidence in the system's security and reduce the risk of security incidents. It is worth noting that the Australian government has taken steps to address the issue of standardization in open banking. For example, the CDR regime, which governs the sharing of consumer data, sets out standards for the secure sharing of financial information. This regime aims to provide consistent standards for the open banking ecosystem and improve the security of sensitive financial information. In sum, while a lack of standardization in open banking can create security risks, standardization could help address these risks and improve the system's security. Further research and empirical data are needed to better understand the relationship between standardization and security in Australia's open banking context.

[83] David Braue, "APRA slams banks for 'inadequate' cyber security," ICT News (July 6, 2023), https://ia.acs.org.au/article/2023/apra-slams-banks-for–inadequate–cyber-security.html.

[84] FinTech Australia, "Submission to the Australian Competition and Consumer Commission Consumer Data Right - Participation of third party service providers" (January 2020), https://www.accc.gov.au/system/files/CDR%20Rules%20-%20intermediaries%20consultion%20submission%20-%20Fintech%20Australia%20REDACT.pdf?ref=0&download=y.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

In terms of open banking regulation, it is assumed that the regulation of open banking in Australia is still in its early stages, and there are some weaknesses in the current regulatory framework. Some of the weaknesses include the following:

- Lack of Oversight: There is limited oversight of third-party providers in the open banking ecosystem, which could potentially lead to security incidents and data breaches. This lack of oversight highlights the need for increased regulatory oversight to ensure the security of sensitive financial information.
- Inadequate Security Standards: While the CDR regime provides some guidelines for the secure sharing of financial information, the security standards may not be comprehensive enough to address all the potential security risks in the open banking ecosystem. These inadequate security standards could leave sensitive financial information vulnerable to attacks.
- Limited Consumer Protection: The current regulatory framework in Australia may not adequately protect consumers using open banking services. For example, there may be limited recourse for consumers who experience financial losses due to security incidents in the open banking ecosystem.
- Inconsistency in Implementation: The implementation of open banking regulations may vary between financial institutions, leading to inconsistent security measures and increasing the risk of security incidents.

Overall, while the current regulation of open banking in Australia has made progress in establishing a framework for sharing consumer data, there are ongoing debates about the strengths and weaknesses of the framework and the need for further improvements. It will be essential to continue monitoring the regulation and making updates as necessary to ensure that it provides adequate consumer protection and promotes a competitive and secure open banking ecosystem.

There is some existing literature that provides limited empirical evidence on the user experience of open banking in Australia. A few studies have been conducted to assess consumer attitudes and behaviors towards open banking.[85] These findings suggest that while there is growing awareness of open banking in Australia, trust in the services is still a significant barrier to adoption. To improve the user experience of open banking, it will be necessary for financial institutions and third-party providers to address consumers' concerns about the security of their financial information and to provide clear and easy-to-use services. In conclusion, further research is needed to better understand the user experience of open banking in Australia and identify ways to improve the adoption and use of these services.

5. Conclusion and Suggestions

From the triangular insight that has been applied, this article argues that open banking has succeeded in offering a new paradigm in the use of banking services in three countries. However, several fundamental concerns still accompany its use. Even though each country has various issues, this article's authors assert that each country needs to strengthen several essential areas. Indonesia, for example, needs to strengthen security concerns, and regulatory authorities in Indonesia need to establish a comprehensive and practical regulatory framework for open banking. This can include measures to ensure the security and privacy of financial data and the implementation of robust security systems and procedures by financial institutions and third-party providers. Concurrently, the Monetary Authority of Singapore (MAS) has implemented a framework for open banking that sets out architectural standards for the secure sharing of financial information. The framework requires financial institutions and third-party providers to implement strong security measures and assess and update these measures regularly. While open banking in Australia offers significant benefits, some potential weaknesses and challenges must be addressed to ensure the framework is implemented effectively, securely, and transparently. In terms of user experience and customer satisfaction in the three countries, the authors suggest the development of several critical indicators, among others, vis-à-vis (a) awareness; (b) trust; (c) convenience; (d) financial inclusion; (e) robust regulation; and (f) further research and data analysis, which is needed to provide a complete picture of adopting open banking services among consumers.

[85] See, e.g., Deloitte, "Open banking: switch or stick? Insights into customer switching behaviour and trust" (October 2019), https://www.ausbanking.org.au/wp-content/uploads/2022/06/Open-Banking-Switch-or-Stick-Insights-Into-Customer-Switching-Behaviour-and-Trust-Deloitte-2019-pdf; Accenture, "Global Banking Customer Study: Reignite human connections to discover hidden value" (2023), https://www.accenture.com/content/dam/accenture/final/industry/banking/document/Accenture-Banking-Consumer-Study.pdf.

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

BIBLIOGRAPHY

Accenture. "Global Banking Customer Study: Reignite human connections to discover hidden value" (2023). https://www.accenture.com/content/dam/accenture/final/industry/banking/document/Accenture-Banking-Consumer-Study.pdf.

Accenture. "Making Digital Banking More Human," 2020 Accenture Global Banking Consumer Survey (2020). https://www.retail-fcl.com/wp-content/uploads/2021/06/Accenture-Banking-Consumer-Study-2020.pdf.

Allen, Hilary J. *et al*. "Regulatory Sandboxes." *George Washington Law Review* 87 (2019): 579–645.

Almehrej, Abdulaziz, Leo Freitas, and Paolo Modesti. *Account and Transaction Protocol of the Open Banking Standard* (Springer, 2020).

Amalia, Camila *et al*. "Legal Issues of Personal Data Protection and Consumer Protection in the Open API Payments." 2 *Journal of Central Banking Law and Institutions* 1 (2022): 323–52.

Asian Banker. "Digitalisation Paving the Way to Financial Inclusion." Finance Indonesia 2022. https://www.theasianbanker.com/finance-indonesia-2022/ (visited 17 April 2024).

"Australia: Internet Penetration 2022." Statista. https://www.statista.com/statistics/680142/australia-internet-penetration/ (visited 17 April 2024).

Australian Banking Association. "Open Banking." https://www.ausbanking.org.au/priorities/open-banking/ (visited 17 April 2024).

Australian Banking Association. "Open Banking Timeline." https://www.ausbanking.org.au/insight/open-banking-timeline/ (visited 17 April 2024).

Australian Government. *Phasing*. Consumer Data Right (Australia, 2020).

"Australian Internet Statistics 2022." Red Search. https://www.redsearch.com.au/resources/australian-internet-statistics/ (visited 24 February 2023).

Ávila, Humberto. *Certainty in Law* (Springer International Publishing, 2016).

Babin, R., and D. Smith. "Open banking and regulation: Please advise the government." 2 *Journal of Information Technology Teaching Cases* 12 (2022): 108–14.

Ball, Christian. "Why Data Has Become Banks Most Important Commodity." *Global Banking & Finance Review* (2017). https://www.globalbankingandfinance.com/why-data-has-become-banks-most-important-commodity/ (visited 17 April 2024).

Bank Indonesia. "Bank Indonesia Launches National Open API Payment Standard and Sandbox Trials of QRIS and Thai QR Payment Interconnectivity" (August 2021). https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2321121.aspx (visited 17 April 2024).

Bank Indonesia. "Blueprint Sistem Pembayaran Indonesia 2025" (2019). https://www.bi.go.id/id/fungsi-utama/sistempembayaran/blueprint-2025/default.aspx.

Billiam, Billiam, Lastuti Abubakar, and Tri Handayani. "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking." 1 *Padjadjaran Jurnal Ilmu Hukum* 9 (2022): 67–88.

Braue, David. "APRA slams banks for 'inadequate' cyber security." ICT News (July 6, 2023). https://ia.acs.org.au/article/2023/apra-slams-banks-for–inadequate–cyber-security.html.

Brick. "Mengenal Open Banking API di Perbankan Indonesia dalam Perkembangan Layanan Finansial" (October 2021). https://www.onebrick.io/id/about/blog/mengenal-open-banking-api-di-perbankan-indonesia-dalam-perkembangan-layananfinan/ (visited 22 July 2022).

Clarke, Gina. "Singapore Launches World's First Public-Private Partnership to Create a New Digital Infrastructure." *Fintech Times* (December 2020). https://thefintechtimes.com/singapore-launches-worlds-first-public-private-partnership-tocreate-a-new-digital-infrastructure/ (visited 17 April 2024).

Competition and Markets Authority UK. "Press Release Update on Open Banking" (2021). https://www.gov.uk/government/news/update-on-open-banking.

Dahdal, A.M., and B. Zeiler. "Open Banking and Open Data: Global Context, Innovation, and Consumer Protection." 7 *Banking Law Journal* 138 (2021): 385–412.

Deloitte. "Open banking: switch or stick? Insights into customer switching behaviour and trust," (October 2019), https://www.ausbanking.org.au/wp-content/uploads/2022/06/Open-Banking-Switch-or-Stick-Insights-Into-Customer-Switching-Behaviour-and-Trust-Deloitte-2019-pdf.

"Digital 2022: Indonesia." DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2022-indonesia (visited 17 April 2024).

"Digital 2022: Singapore" (9 February 2022). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital2022-singapore (visited 17 April 2024).

Dong, Chengzu *et al*. "BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity" (Springer Science and Business Media Deutschland GmbH, 2020).

Eroglu, Hakan *et al*. "PSD2 & Open Banking Security and Fraud Impacts on Banks Are You Ready?" (Accenture, 2016).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

European Central Bank. "The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security" (2018). https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

Farrell, Scott. "Banking on Data: A Comparative Critique of Common-law Open Banking Frameworks." PhD Thesis. The University of New South Wales (2022). https://doi.org/10.26190/unsworks/24096.

Farrell, Scott. "The State of Open Banking in Australia in 2021" (2021). https://thepaypers.com/expert-opinion/the-state-ofopen-banking-in-australia-in-20211253611-#:~:text=Australian%20Open%20Banking%20is%20up,as%20well%20as%20transaction%20accounts.

Finastra. Press Release. "Finestra global survey shows appetite for open finance in Singapore against back drop of constrained investment" (December 7, 2022). https://www.finastra.com/sites/default/files/file/2022-12/Press%20release_State-of-the-Nation-Research_Sing_final.pdf.

FinTech Australia. "Submission to the Australian Competition and Consumer Commission Consumer Data Right – Participation of third party service providers" (January 2020). https;//www.accc.gov.au/system/files/CDR%20Rules%20-%20intermediaries%20consultion%20submission%20-%20Fintech%20Australia%20REDACT.pdf?ref=0&download=y.

Fintech Singapore. "What Does Singapore's Open Banking Landscape Look Like in 2021?" (30 June 2021). Fintech Singapore. https://fintechnews.sg/52211/openbanking/what-does-singapores-open-banking-landscape-look-like-in-2021 (visited 17 April 2024).

Frollo and NextGenNet. "The State of Open Banking Report 2020" (2020). https://frollo.com.au/open-banking/state-of-openbanking-report-2020/ (visited 17 August 2022).

Galdikas, Marius. "Does Open Banking Live Up to Its Claims? Key Aspects that Hinder Smooth Transactions" (February 2022). https://thepaypers.com/thought-leader-insights/does-open-banking-live-up-to-its-claims-key-aspects-that-hinder-smoothtransactions–1254627 (visited 17 April 2024).

Gauci, Rachel. "Is Europe a Good Example of Open Banking?." In *The PayTech Book*, edited by S. Chishti *et al*. (Wiley, 2020). https://doi.org/10.1002/9781119551973.ch25.

Government Technology Agency Singapore, "SingPass - Singapore"s National Digital Identity" (Sep. 18, 2024), https://www.singpass.gov.sg/main/trusted-identity.

Hantrais, Linda, and Ashley Thomas Lenihan. "Social dimensions of evidence-based policy in a digital society." 2 *Contemporary Social Science* 16 (2021): 141–55.

Hermawan, Sapto *et al*. Singapore Government Developer Portal. "API Exchange (APEX) - A Centralised Data Sharing Platform for the Public Sector" (October 2022). https://www.developer.tech.gov.sg/products/categories/data-and-apis/apex/overview.html (visited 17 April 2024).

KPMG. "Global Banking Fraud Survey: The multi-faceted threat of fraud: Are banks up to the challenge?" (May 2019).

Leong, Emma. "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia and Singapore." 35.3 *Banking & Finance Law Review* (2020): 443–69.

Lynn, Theo, Pierangelo Rosati, and Mark Cummins. "Exploring Open Banking and Banking-as-a-Platform: Opportunities and Risks for Emerging Markets." In *Entrepreneurial Finance in Emerging Markets*, edited by Darek Klonwski (Palgrave Macmillan, 2020).

Madir, Jelena, ed. *Fintech Law and Regulation*. 2nd ed. (Elgar, 2021).

Mansfield-Devine, Steve. "Open banking: opportunity and danger," 2016 *Computer Fraud & Security* 10 (2016). https://www.sciencedirect.com/science/article/pii/S136137231630080X.

Ministry of Foreign Affairs of the Netherlands. "The Role of Consumer Consent in Open Banking" (2021).

Monetary Authority of Singapore. "API Exchange (APIX)" (2021). https://www.mas.gov.sg/development/fintech/api-exchange (visited 26 July 2022).

Monetary Authority of Singapore. "Financial Industry API Register." https://www.mas.gov.sg/development/fintech/financial-industry-api-register (visited 17 April 2024).

Monetary Authority of Singapore. "Digital Infrastructure to Enable More Effective Financial Planning by Singaporeans" (7 December 2020). https://www.mas.gov.sg/news/media-releases/2020/digital-infrastructure-to-enable-more-effectivefinancial-planning-by-singaporeans (visited 17 April 2024).

Monetary Authority of Singapore and Association of Banks in Singapore. ABS-MAS Financial World | Finance-as-a-Service: API Playbook (2016).

Murinde, Victor, Efthymios Rizopoulos, and Markos Zachariadis. "The Impact of the FinTech Revolution on the Future of Banking: Opportunities and Risks." *International Review of Financial Analysis* 81 (2022): 102103.

NACHA (Electronic Payments Association). "API Standardization-Shaping the Financial Services Industry" (2018). https://smallake.kr/wp-content/uploads/2019/05/707-18-4-API-Standardization-Shaping-the-Financial-Services-Industry.pdf.

OECD. Data Portability in Open Banking Privacy and Other Cross-cutting Issues (2023). https://www.oecd.org/digital/dataportability-in-open-banking-6c872949-en.htm.

OECD. Digital Disruption in Banking and its Impact on Competition (2020).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press

Open Banking Limited. "Three Years since PSD2 Marked the Start of Open Banking, the UK Has Built a World-leading Ecosystem" News (13 January 2021). https://www.openbanking.org.uk/news/three-years-since-psd2-marked-the-start-ofopen-banking-the-uk-has-built-a-world-leading-ecosystem/ (visited 17 April 2024).

Open Banking Limited. *Annual Report* 2020 (London: Open Banking Limited, 2020).

Otoritas Jasa Keuangan, Republik Indonesia. Digital Finance Innovation Road Map and Action Plan 2020–2024 (2020).

"Quarterly Digital Briefings." Kepios. https://kepios.com/briefings (visited 17 April 2024).

Remolina, Nydia. "Open Banking: Regulatory Challenges for A New Form of Financial Intermediation in A Data-driven World." SMU Centre for AI & Data Governance Research Paper no. 2019/05 (2019). https://ssrn.com/abstract=3475019.

Reynolds, Faith. "Open Banking: A Consumer Perspective." Barclays (2017). https://home.barclays/content/dam/home-barclays/documents/citizenship/access-to-financial-and-digital-empowerment/Open-Banking-A-Consumer-Perspective-Faith-Reynolds.pdf.

Reynolds, Faith *et al*. "Consumer Priorities for Open Banking" Openbanking.org (2019). https://www.openbanking.org.uk/wp-content/uploads/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf.

Ridings, Liam. "Australian Internet Statistics 2022 – Essential Facts and Stats" Safari Digital (16 May 2021). https://www.safaridigital.com.au/blog/australian-internet-statistics (visited 24 February 2023).

Selmer, Roland. "Insight: Why Momentum Tells the True UK Open Banking Success Story." Open Banking Expo (March 2022). https://www.openbankingexpo.com/insights/insight-why-momentum-tells-the-true-uk-open-banking-success-story/ (visited 17 April 2024).

"Statistik Fintech Lending Periode Maret 2022." https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik Fintech-Lending-Periode-Maret-2022.aspx (visited 17 April 2024).

"Studi Dampak Fintech Peer-To-Peer Lending Terhadap Perekonomian Nasional." INDEF. https://indef.or.id/en/publikasi/studidampak-fintech-peer-to-peer-lending-terhadap-perekonomian-nasional/ (visited 17 April 2024).

Sugarda, Paripurna P., and Muhammad Rifky Wicaksono. "Enhancing the Competitiveness of Indonesia's Financial Services Sector in the Digital Era Through Open Banking: Lessons Learned From the UK's Experience." *Journal of Central Banking Law and Institutions* 2, no. 1 (2023): 153–78.

Tsai, C-H, and K-J Peng. *Regulating open banking: Comparative analysis of the EU, the UK and Taiwan* (Routledge, 2022).

Zachariadis, Markos, and Pinar Ozcan. "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking." Swift Institute Working paper no. 2016-001. (2017).

https://doi.org/10.1017/jli.2024.11 Published online by Cambridge University Press