1-2021

Shifting contour of data sharing in financial market and regulatory responses: The UK and Australian models

Han-wei LIU
Singapore Management University, hanweiliu@smu.edu.sg

SHIFTING CONTOUR OF DATA SHARING IN FINANCIAL MARKET AND REGULATORY RESPONSES: THE UK AND AUSTRALIAN MODELS

HAN-WEI LIU*

* Senior Lecturer, Monash University, Australia. The author is grateful to Tiana Moutafis and Lily Raynes for excellent research assistance and wishes to thank the editorial team of *American University Business Law Review*, in particular, Alex and Monica, for their support throughout the process. The remaining errors are mine alone.

I. INTRODUCTION

Starting from Directive 2015/2366 on Payment Services in the Internal Market[1] — known as PSD II in the European Union (EU) — countries across the world have or are contemplating a new framework to govern data sharing among different players in the financial market. "Open Banking," as this trend is called, requires or encourages — depending on the regulatory models adopted in different jurisdictions — banks to share consumer-permissioned banking data with third parties securely, in a form that facilitates its use.[2] The Open Banking initiatives have diffused from the EU, and the UK, to elsewhere. The current Open Banking trend raises analytical questions: is data sharing novel in the banking sector? Before introducing Open Banking, did banks share their data with third parties, and if so, how? On the other hand, however, if data sharing did exist in the pre-Open Banking world, why would governments ever bother to introduce the Open Banking initiatives at all? What are the rationales or concerns justifying such regulatory intervention? What do these regulatory responses look like, and how effective are they in reacting to these concerns?

This Article seeks to contribute to the existing literature by addressing these questions through a comparative lens. For our present purpose, we focus on Open Banking initiatives in the UK and Australia. The former is widely seen as a pioneer in Open Banking by rolling out its regime in 2018,[3] while Australia is the first to launch a comprehensive data-sharing regime across the whole economy.[4] Both could serve as a template for other jurisdictions to articulate their regimes. Analyzing key aspects of the regulatory designs of these two models not only underscores the major differences and the rationales underpinning them but also helps inform other countries to configure or reflect upon their regulatory schemes when

1. Directive (EU) 2015/2366, of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, 2015 O.J. (L 337) 35 [hereinafter PSD II].

2. *See UK's Open Banking to Launch on 13 January 2018*, OPEN BANKING IMPLEMENTATION ENTITY (Dec. 19, 2017), https://www.openbanking.org.uk/about-us/latest-news/uks-open-banking-launch-13-january-2018/ ("Open Banking is a term that describes a secure set of technologies and standards that allow customers to give companies other than their bank or building society permission to securely access their accounts.").

3. *See id.* ("[T]he UK will be the first nation to launch Open Banking when its service goes live in early 2018.").

4. *See* Victor Chatenay, *Australia Has Rolled Out an Open Banking Regime*, BUS. INSIDER (July 6, 2020, 9:36 AM), https://www.businessinsider.com/australia-open-banking-regime-goes-live-2020-7 (noting that on July 1, 2020, Australia's Consumer Data Right Act became law and will continue to be implemented across different sectors of the economy in stages).

introducing similar data-sharing initiatives.

Against this background, this Article proceeds as follows. Part II sets the stage by unpacking the trajectory of data-sharing in the banking sector and the underlying concerns that lead to regulatory responses via Open Banking initiatives. Part III then examines in-depth the selected issues around Open Banking, including the participants, the scope of data to be shared, liabilities arising from authorized transactions, measures dealing with security and data protection concerns, and the legality of screen scraping after Open Banking. Part IV concludes.

II. OPEN BANKING: ORIGIN, RATIONALES, AND NORM DIFFUSION

A. Data Sharing in Banking Sector: A Shifting Landscape

Banks in most jurisdictions are subject to a legal obligation — by way of contracts, statutes, or case law — to maintain "bank secrecy" or "bank confidentiality" and conceal clients' information.[5] By virtue of clients' consent or otherwise, banks could share consumers' information with third parties. Data sharing between banks and third parties might proceed through either contractual arrangements or technologies. On the former, one oft-seen arrangement is between a bank and a credit bureau to evaluate the creditworthiness of prospective or existing customers.[6] Of particular note is the latter — data sharing through so-called "screen scraping," a process by which automated scripts extract portions of data from one application for another to use.[7] When screen scraping, a third party has access to a clients' account credentials. By virtue of this insight, said third party can unearth additional data without involving or alerting the bank where the account is

5. Traditionally, contract law is the most important source governing bankers' duty of secrecy. Where the contract is silent, this duty is interpreted by the courts to be an implied term between a bank and its customer. Tournier v. Nat'l Provincial & Union Bank of England, [1924] 1 KB 461 (Bankes LJ). *See generally* Dora Neo, *A Conceptual Overview of Bank Secrecy*, *in* CAN BANKS STILL KEEP A SECRET? 3–30 (Sandra Booysen & Dora Neo eds., 2017) (noting how banks are prohibited from disclosing their clients' information in different countries).

6. *See, e.g.*, HSBC, CREDIT INFORMATION MANAGEMENT POLICY (2020), https://www.hsbc.com.au/content/dam/hsbc/au/docs/pdf/hsbc-credit-policy.pdf (explaining that credit information is important to determining credit worthiness and how credit information may be used in the process).

7. BASEL COMM. ON BANKING SUPERVISION, REPORT ON OPEN BANKING AND APPLICATION PROGRAMMING INTERFACES 19 (2019) [hereinafter BASEL COMM., REPORT ON OPEN BANKING]; *see* GoCardless, *Screen Scraping 101: Who, What, Where, When?*, THE OPEN BANKING HUB (July 19, 2017), https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712 (describing how services use screen-scrapping to access a user's banking information, such as their last transaction, and the potential associated risks).

located.[8]

Screen scraping is nothing new. It closely relates to the emergence of "data aggregation" (also known as "account aggregation," or "financial aggregation" as applied in the financial sector) some two decades ago. Data aggregation services were first offered in the United States in the late 1990s.[9] Such services catalogue clients' account information from various institutions in a central location; these service providers collate consumers' financial data relating to, among other things, their "deposit accounts, credit accounts, managed funds accounts, and[] brokerage accounts."[10] They also collate non-financial data (e.g., those from email accounts).[11] This business model has since diffused throughout Europe and the Asia Pacific.[12] As early as 2000, for instance, Australia had seven firms providing data aggregation services: two associated with financial institutions, and one provided by a stockbroker.[13] More recently, Fintech firms have been tapping into the potential of data by purchasing data made available by data aggregators and then using it to offer new products and services.[14] Another technique employed by third parties in recent years is reverse engineering, which extracts information about the source code of mobile banking applications to determine which information is exchanged between the bank's server and the applications.[15] As it is more robust and generally unaffected by changes to the bank's interface, data aggregators typically prefer reverse engineering to screen scraping.[16]

---

8. AUSTL. SEC. & INV. COMM'N, CONSULTATION PAPER 20: ACCOUNT AGGREGATION IN THE FINANCIAL SERVICES SECTOR 15 (2001) [hereinafter ASIC CONSULTATION PAPER 20].

9. *See id.* at 1.

10. *Id.* at 7.

11. *Id.*

12. *See, e.g.*, Hiroshi Fujii et al., *E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific* (Composite Info. Sys. Lab'y, Mass. Inst. of Tech. Sloan Sch. of Mgmt., Working Paper No. 2002-06, 2002), http://web.mit.edu/smadnick/www/wp/2002-06.pdf.

13. *See* ASIC CONSULTATION PAPER 20, *supra* note 8, at 17–18 (illustrating the results of the aggregation services provider study).

14. *See* Brian J. Hurh et al., *Consumer Financial Data Aggregation and the Potential for Regulatory Intervention*, 71 CONSUMER FIN. L. Q. REP. 20, 21 (2017) (noting that with the acquired data, the offered products and services can be "more targeted and tailored" to the consumer).

15. *See* THE AUSTL. GOV'T THE TREASURY, REVIEW INTO OPEN BANKING: GIVING CUSTOMERS CHOICE, CONVENIENCE AND CONFIDENCE 72 (Dec. 2017) [hereinafter THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING], https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

16. *See* BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 9 (acknowledging, however, that both techniques still pose risks to the customer because

The underlying concerns around screen scraping or reverse-engineering have led banks to introduce their application programming interfaces ("APIs") — a standardized communication method that enables data flow between systems in a seamless yet controlled way.[17] The degree of openness of these interfaces may vary, such as the level of protection, the bank's duty towards clients, and the bank's ability to compete with outside developers.[18] Banks lacking budgets and expertise to develop their APIs may instead engage data aggregators as middlemen by contracts.[19]

B. Rationales for Data Sharing: Benefits and Concerns

Data sharing presents advantages and disadvantages for different stakeholders in the financial industry. An advantage is that it could give consumers more control over when and what data is shared with third parties — be they banks, other financial institutions, or Fintech start-ups — in search of better, personalized deals, thereby improving personal finance decisions.[20] Examples are countless. The platform of Akoni, a British firm, helps companies maximize the return on their deposits and provides personalized cash tips and benchmarks reflecting similarly sized companies.[21] By making the market transparent and increasing the variety of choices available, data sharing helps reshape the banking industry — at least in retail banking — where clients often display "stickiness" to an incumbent due to switching

---

the data aggregator retains access to the customer's account and may perform unauthorized actions, such as engaging in a financial transaction).

17. Penny Crosman, *Wells Fargo's Bid to Vanquish Screen Scraping*, AM. BANKER (June 7, 2016, 6:30 AM), https://www.americanbanker.com/news/wells-fargos-bid-to-vanquish-screen-scraping ("APIs connect servers in a way that avoids all the problems of screen scraping — the sharing of user names and passwords, the overloading of banks' servers with high-volume requests, the inability to use two-factor authentication.").

18. Lael Brainard, Governor, Fed. Rsrv. Sys., Speech at the Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice": Where Do Banks Fit in the Fintech Stack? (Apr. 28, 2017), https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm.

19. *Id.*

20. *See id.* (suggesting that "screen scraping . . . may be the most effective tool for the customers of small community banks to access the financial apps they prefer" and thus, a necessary tool "to remain competitive until more effective broader industry solutions are developed").

21. *See, e.g.*, *Frequently Asked Questions*, AKONI, https://akonihub.com/static/faq (last visited July 10, 2021).

costs.[22] Data sharing can, in other words, help fix the "lock-in" problem,[23] addressing concerns that banks' information monopoly can victimize Fintech start-ups via anti-competitive practices.[24] With better data access, one report shows that Australians could save up to $11.6 billion AUD annually by switching service providers.[25] Another benefit is that the "growth in volume, variety, and sources of data" can reduce barriers to entry, this is particularly advantageous for new firms with innovative plans for this novel information."[26]

As promising as data sharing can be, however, there are concerns around the current practice. First, it is not uncommon for banks to overlook the opportunities that come with data sharing and instead perceive it as a threat to their fundamental values,[27] raising concerns that they would be recast as an involuntary "platform as a service" ("PaaS") provider and compelled to face fiercer competition to maintain their clients.[28] Incumbents are also concerned with the level playing field: what are the obligations imposed onto these Fintech start-ups when traditional banks are forced or "nudged" to

22. *See* Alasdair Smith, CMA Inquiry Chair, Speech at the BBA Retail Banking Conference on Competition and Open Banking (June 29, 2017), https://www.gov.uk/government/speeches/alasdair-smith-on-competition-and-open-banking (explaining the difficulties consumers may have accessing information and how "opening banking" can help remedy this information gap).

23. Giuseppe Colangelo & Oscar Borgogno, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule* 7 (Stanford — Vienna Transatlantic Tech. L. F., EU Law Working Papers, Paper No. 35, 2018) (explaining "lock-in problems" and their effect on the banking industry).

24. AUSTL. GOV'T PRODUCTIVITY COMM'N, REP. NO. 82, DATA AVAILABILITY AND USE 567 (2017) [hereinafter PRODUCTIVITY COMM'N (AUSTL.), DATA AVAILABILITY AND USE] (noting that data sharing "would almost certainly" encourage efficient competition to the benefit of consumers); Colangelo & Borgogno, *supra* note 23, at 10 ("[F]ront-end providers are more prone to be victims of anti-competitive practices carried out by banks and other incumbents than end-to-end providers.").

25. PRODUCTIVITY COMM'N (AUSTL.), DATA AVAILABILITY AND USE, *supra* note 24, at 101.

26. *Id.* at 553.

27. *See* ACCENTURE, THE BRAVE NEW WORLD OF OPEN BANKING 5 (2018); Daniel Ziffer, *Open Banking Will Threaten the Dominance of the Big Four Banks — But It Has Been Delayed*, ABC NEWS, (Dec. 20, 2019, 8:27 PM), https://www.abc.net.au/news/2019-12-20/open-banking-revolution-to-shake-up-the-dominance-of-big-four/11813498.

28. *See* Colangelo & Borgogno, *supra* note 23, at 21 (explaining different ways "banks are likely to [fiercely] compete . . . to attract as many new customers and third-party providers as possible"); Jane K. Winn, Reengineering European Payment Law 27 (June 30, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3412457 (explaining the disadvantages to banks resulting from being classified as PaaS providers).

assume this new role as a PaaS provider?[29] Second, while screen scraping or reverse-engineering represents a less costly approach for third parties to access consumers' data, these techniques have pitfalls from a technical perspective. Screen scraping, for instance, does not guarantee data accuracy or currency, as banks may reconfigure their settings from time to time.

Moreover, the data collected by third parties could be stolen or misused for payment fraud.[30] Banks may find it problematic to distinguish between consumers, aggregators, and unauthorized third parties when someone logs onto the account.[31] These practices could also arguably burden a bank's IT system by extracting a large amount of data.[32] Other concerns are cybersecurity,[33] data breach (e.g., whether the third parties can pass the information to fourth parties and beyond),[34] and of course, the allocation of liability arising from unauthorized transactions.[35] Furthermore, while many jurisdictions do not explicitly ban screen scraping or reverse engineering, these techniques have, as a matter of practice, created controversy in various jurisdictions — *American Airlines, Inc. v. FareChase, Inc.*[36] and *eBay, Inc. v. Bidder's Edge, Inc.*[37] in the United States,[38] and *Ryanair Ltd. v Bravofly*[39]

29. Winn, *supra* note 28, at 27.

30. BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 9.

31. *Id.* (acknowledging that this is done when third parties store customer credentials, thus giving them access to the customer's account).

32. *Id.* (noting that the third-party data aggregators may "extract large volumes of data at multiple intervals").

33. *See, e.g.*, ASIC CONSULTATION PAPER 20, *supra* note 8, at 46 (referring to one U.S. commentator's report that appropriate agreements should be signed between banks and data aggregators to address privacy and security concerns).

34. BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 12 (cautioning that third parties may use or share the customer's information beyond the scope of the customer's consent).

35. *Id.* at 14 (stating that liability laws may be unable to properly determine liability in an open banking or data sharing dispute).

36. Temporary Injunction at 2–4, Am. Airlines, Inc. v. FareChase, Inc., No. 067-194022-02 (67th Dist. Ct. Tarrant Cty., Tex. Mar. 8, 2003).

37. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

38. One recurring issue in the United States is whether the trespass-to-chattels doctrine would apply to screen scraping. Temporary Injunction at 4, *Am. Airlines, Inc.*, No. 067-194022-02 (granting a temporary injunction to ban, among others, Farechase from using software to obtain and copy data from American Airlines' system); *eBay, Inc.*, 100 F. Supp. 2d at 1063–65 (moving for a preliminary injunction to prevent Bidder's Edge from further accessing eBay's system after Bidder's Edge accessed it approximately 100,000 times a day). For a comparative study of the legality of screen scraping in the United States, the United Kingdom, and Australia, see generally Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and its Open Banking Watershed Moment*, 30 WASH. INT'L L.J. 28 (2020).

39. Ryanair Ltd v. Bravofly [2009] IEHC 224. Ryanair claimed, among others, that

in Ireland, are cases in point.

C. A Snapshot of Global Normative Diffusion of Open Banking: EU and Beyond

The EU was the first jurisdiction mandating access to account data by Directive 2015/2366 on Payment Services in the Internal Market — known as PSD II.[40] EU Member States were required to transpose the PSD II into national law by January 13, 2018.[41] To date, all EU Members have acted accordingly.[42] PSD II was built on its predecessor, the first Payment Systems Directive ("PSD I"),[43] adopted in 2007 as the foundation to establish safer and more innovative payment services across the single market.[44] The revisions by PSD II represents an effort to adapt to the evolving technology in the payment services market and its associated challenges.

PSD II applies to all payment service providers ("PSPs"); it is a broad term that encompasses both banks and various third parties providing selected financial services (including account information and payment initiation services).[45] It obliges banks to provide a customer's data to authorized third parties in specified circumstances.[46] Such third parties are either Payment Initiation Service Providers ("PISPs")[47] or Account Information Service Providers ("AISPs"),[48] collectively known as Third-Party Providers ("TPPs"). Generally, PISPs expedite online transactions by allowing consumers to directly execute an online payment from their accounts and offer cost-effective solutions for both merchants and consumers.[49] For example, Banked is a UK-authorized fintech company[50] that allows a

Bravofly's practice of screen-scraping breaches Ireland's Trademarks Act and the Copyright and Related Rights Act and violated the terms and conditions of using Ryanair's website.

40. Directive (EU) 2015/2366, of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, 2015 O.J. (L 337) 35.

41. *Id.* art. 109 at 111.

42. *Payment Services (PSD2) — Transposition Status*, EUR. CMM'N, https://ec.europa.eu/info/publications/payment-services-directive-transposition-status_en (last updated May 5, 2021).

43. Directive 2007/64/EC, of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market, 2007 O.J. (L 319) 1.

44. *Id.* recital 4 at 1.

45. PSD II, *supra* note 1, arts. 1, 4(3), 4(11), annex I, at 53–54, 57, 116.

46. *Id.* arts. 2, 66–67 at 54, 92–93.

47. *Id.* art. 66 at 92–93.

48. *Id.* art. 67 at 93.

49. *Id.* art. 4 at 57–60; *id.* recital 28 at 39.

50. *Financial Services Register*, FIN. CONDUCT AUTH., https://register.fca.org.uk/s/firm?id=0010X00004EMNS0QAP (last visited July 10, 2021).

merchant to share its financial details and request payment, with the customer then authorizing this transfer of funds.[51] AISPs consolidate data across different clients' accounts, giving them a better overview of their financial situation.[52] This can help facilitate the development of other services in the Fintech ecosystem[53] — for example, Bippit compiles a customer's information and shares it with a financial adviser so they can advise clients virtually.[54] Due to their different functions, PISPs are often described as having "read-write" access, while AISPs have "read-only" access.[55]

Central to the PSD II is consent: for a TPP to access a customer's data (or "payment service user"), it must obtain their explicit consent.[56] Upon receiving the customer's consent, the bank must securely communicate with the PISP or AISP to provide the necessary data,[57] regardless of whether they have a pre-existing contractual relationship with that TPP.[58] Therefore, the framework empowers bank customers to retrieve their data as easily as they can access the funds in their accounts, making it available to Fintech firms in exchange for new services.[59]

By freeing up data, PSD II is the first regime that definitively opens up the payment services market to TPPs other than banks.[60] The underlying rationale is, as mentioned above, to increase competition in the industry by

51. David Kimberly, *Faster, Safer: Payments Under Open Banking*, FIN. MAGNATES (Aug. 16, 2019, 11:01 AM), https://www.financemagnates.com/fintech/payments/faster-safer-payments-under-open-banking/.

52. PSD II, *supra* note 1, recital 28, art. 4, at 39, 53–54 (defining and explaining the technology that gives customers an overview of their financial situation).

53. *8 Frequently Asked Questions About Account Information Service Providers*, FINTEC SYS. (Oct. 5, 2018), https://knowledge.fintecsystems.com/en/blog/8-frequently-asked-questions-about-account-information-service-providers (describing AISPs and their impact on the Fintech Industry).

54. *How It Works*, BIPPIT, https://bippit.com/how-it-works/ (last visited July 13, 2021).

55. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 2, 108; Kelly Read-Parish, *Open Banking: AISPs and PISPs Explained*, FINEXTRA (Feb. 11, 2019), https://www.finextra.com/blogposting/16647/open-banking-aisps-and-pisps-explained.

56. PSD II, *supra* note 1, art. 64(1) at 91.

57. *Id.* arts. 66–67 at 92–93; *see also infra* Part III.B.

58. PSD II, *supra* note 1, arts. 66(5), 67(4) at 92–93.

59. Fernando Zunzunegui, *Digitalisation of Payment Services* 16 (Ibero-American Inst. for L. & Fin., Working Paper No. 5/2018, 2018) (noting that access to this data can be quite valuable for customers).

60. PSD II has gone further than PSD I by permitting non-bank firms to use not only "payment institution" status, but also "PISP" or "AISP" status. *Id.* at 24–25.

bringing innovative players into the market.[61] Also, PSD II addresses some of the concerns around data sharing examined earlier: it can create a more integrated payment market with common standards, increase the safety and security of payments, and protect consumer data in an Open Banking system where self-regulation may be insufficient.[62]

In implementing PSD II, the UK was the first to offer a governmental program to work toward Open Banking.[63] Her Majesty's Treasury in 2015 announced its commitment to delivering an open standard for APIs and data sharing in the UK retail banking sector to increase the opportunities for competition, thereby improving outcomes for customers in the banking industry.[64] This implementation was achieved in 2018 by the Retail Banking Market Investigation Order 2017,[65] issued by the Competition and Markets Authority ("CMA").[66] This CMA Order applies to the nine largest banks in the UK,[67] requiring them to make certain data available via an API to authorized third parties.[68]

While these European initiatives may represent the "cradle of Open Banking," the practice has since been adopted in other jurisdictions in their forms.[69] The most notable example is Australia, which recently rolled out

61. *See European Parliament Adopts European Commission Proposal to Create Safer and More Innovative European Payments*, EUR. CMM'N (Oct. 8, 2015) [hereinafter EUR. COMM'N, *Safer and More Innovative European Payments*], https://ec.europa.eu/commission/presscorner/detail/ro/IP_15_5792 (stating that these innovations will provide protection for European customers); OPEN BANKING IMPLEMENTATION ENTITY, OPEN BANKING: GUIDELINES FOR OPEN DATA PARTICIPANTS 3 (2018) [hereinafter OBIE, GUIDELINES FOR OPEN DATA PARTICIPANTS], https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Open-Data-Participants.pdf (detailing how open banking operates to bring new players into the market).

62. *See* Zunzunegui, *supra* note 59, at 27; EUR. COMM'N, *Safer and More Innovative European Payments*, *supra* note 61 (outlining changes to the regulations brought by PSD II).

63. Zunzunegui, *supra* note 59, at 15.

64. HM TREASURY (U.K.), DATA SHARING AND OPEN DATA IN BANKING: RESPONSE TO THE CALL FOR EVIDENCE 7 (2015) (concluding that given the noted benefits the government is "commit[ed] to deliver[ing] and open API standard in UK banking").

65. Retail Banking Market Investigation: The Retail Banking Market Investigation Order 2017 (UK) [hereinafter UK CMA Order].

66. *Id.* § 2.9.

67. *Id.* § 3.1.1 (listing RBSG, LBG, Barclays, HSBCG, Nationwide, Santander, Danske, Bol, and AIBG as the nine largest UK banks).

68. *Id.* § 2; *Third Party Providers*, OBIE [hereinafter OBIE, *Third Party Providers*], https://www.openbanking.org.uk/providers/third-party-providers/ (last visited Apr. 24, 2021) (detailing the steps required to become a provider); *see also infra* Part III.A–B.

69. *See* EMEA Center for Regulatory Strategy, *Open Banking Around the World*, DELOITTE, https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html (last visited July 13, 2021) (summarizing open banking models outside of the EU and noting there are two general categories: "market-driven"

its Open Banking regime as part of the broader Consumer Data Right ("CDR"). CDR is unique because it is broadly framed as a data policy initiative rather than a financial service one,[70] and while it will apply first to banks, it will gradually be rolled out to the whole economy. [71]

The regime was passed on August 1, 2019, in the Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth) ("CDR Act").[72] However, the Australian Competition and Consumer Commission ("ACCC") pushed back its roll-out from February to July 2020 as a result of incomplete tests.[73] The CDR roll-out emerged as a response to several reviews, including one by the Australian Productivity Commission in 2017[74] and one by the Farrell Review in the same year.[75] Notably, CDR works towards a comprehensive data access regime, furthering the existing data access rules set forth under the Australian Privacy Principles ("APPs").[76] Among others, the regime requires data-holders (e.g., banks) to securely transfer a customer's data, upon request, to an accredited third party. Like its UK/EU counterpart, CDR intends to encourage competition, enhance consumer welfare, reduce switching costs, and enable a range of business opportunities to emerge from data sharing.[77]

---

or "regulatory-driven").

70. *Id.* (noting that as a data policy initiative, it could be implemented in any industry of the economy).

71. Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) 5, 7 (Austl.) [hereinafter Explanatory Memorandum, CDR Bill] (emphasizing the Government's dedication to applying CDR across various sectors of the economy, such as "the energy and telecommunications sectors").

72. This Act amended the *Competition and Consumer Act 2010* (Cth) (Austl.), *Australian Information Commissioner Act 2010* (Cth), and *Privacy Act 1988* (Cth) (Austl.) to create the Consumer Data Right.

73. Press Release, Austl. Competition & Consumer Comm'n, Consumer Data Right Timeline Update (Dec. 20, 2019) [hereinafter ACCC, CDR Timeline Update], https://www.accc.gov.au/media-release/consumer-data-right-timeline-update (citing the ACCC's dedication to ensuring a user-friendly system and "robust privacy protection" as the reason for postponing the launch).

74. PRODUCTIVITY COMM'N (AUSTL.), DATA AVAILABILITY AND USE, *supra* note 24, at 35 (recommending the creation of an economy-wide Consumer Data Right).

75. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 11, 13–14 (recommending that Open Banking be implemented through the broader CDR framework). A Senate Committee is also currently conducting an inquiry into the future direction of the CDR framework, including potential "write-access" in the banking sector (for payment initiation) and roll-out to the superannuation sector. SENATE SELECT COMM. ON FIN. TECH. & REGUL. TECH., PARLIAMENT OF AUSTRALIA, ISSUES PAPER 9 (2019).

76. *See infra* Part III.B.

77. Explanatory Memorandum, CDR Bill, *supra* note 71, at 5 (outlining the aims and values of the CDR).

Conceptually, the approaches adopted by different jurisdictions fall within one of the following camps. Some of them — like the EU, UK, and Australian schemes — follow the mandatory (or prescriptive) approach by laying down a comprehensive framework of Open Banking.[78] Others take the voluntary (or facilitative) model via guidelines, standards, and technical specifications on APIs to assist data sharing.[79] The "Finance-as-a-Service: API Playbook" issued by the Monetary Authority of Singapore and the Association of Banks in Singapore,[80] and the "Open API Framework for the Hong Kong Banking Sector" released by Hong Kong Monetary Authority,[81] are prime examples. Still, in other jurisdictions, there is currently no regulatory framework to mandate or facilitate Open Banking, although there has been discussion on the subject. In the United States, for instance, it is heatedly debated as to whether Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act can serve as a vehicle to require financial institutions to share consumer data with TPPs.[82] With this backdrop, we now turn to examine the regulatory approaches dealing with specific concerns around data sharing in the UK and Australia below.

III. A COMPARATIVE ANALYSIS OF AUSTRALIA AND THE UK

A. Who Can Participate?

In the UK, the CMA Order applies to the nine largest banks — known as the "CMA9" — requiring them to make certain data available through an

78. BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 11–12 (describing the mandatory and formal nature of the EU, UK, and Australian frameworks).

79. *Id.* (highlighting Hong Kong and Singapore as examples of countries employing the facilitative model).

80. ASS'N OF BANKS & MONETARY AUTH. OF SINGAPORE, FINANCE-AS-A-SERVICE: API PLAYBOOK (2016).

81. HK MONETARY AUTH., OPEN API FRAMEWORK FOR THE HONG KONG BANKING SECTOR (2018) (detailing the regulatory framework set for the Hong Kong banking sector).

82. *See, e.g.*, Michael S. Barr et al., *Consumer Autonomy and Pathways to Portability in Banking and Financial Services* 3 (Ctr. on Fin., Law & Policy, Univ. Mich. Working Paper No. 01, 2019), http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf ("Section 1033 of the Dodd-Frank Act grants consumers the right to access their personal financial information. But there is significant dispute about the scope of § 1033 . . . ."); Mary Wisniewski, *The Data Access Debate Is About to Get A Lot More Interesting*, AM. BANKER (Jan. 27, 2017, 3:27 PM), https:/www.americanbanker.com/news/the-data-access-debate-is-about-to-get-a-lot-more-interesting (noting that some interpret § 1033 as only "contemplate[ing] a direct relationship between a customer and bank" while others argue that it "codif[ies] consumers' right to access their financial data through third-party apps").

API.[83] Non-CMA9 providers may also voluntarily participate in Open Banking. To access data via the banks' APIs, TPPs must be eligible under the PSD II so they can obtain authorization from the Financial Conduct Authority ("FCA").[84] Upon being granted such regulatory permission, TPPs are placed on a "whitelist" — known as the Open Banking Directory, as maintained by the Open Banking Implementation Entity ("OBIE"),[85] to provide services using Open Banking.[86]

In Australia, the CDR regime will apply to, in the case of the banking sector, all authorized deposit taking institutions ("ADIs") other than foreign banks.[87] However, implementation will be phased in, with trials by the four largest banks — ANZ, Commonwealth, Westpac, and NAB.[88] These major banks are required to provide access to customer data under the CDR by July 2020;[89] other ADIs must do so by July 2021.[90] Moreover, to receive such data, TPPs must become "Accredited Recipients"[91] by meeting certain criteria, including privacy and security requirements.[92]

B. What Data Should Be Shared?

The scope of data sharing may vary depending on jurisdiction. Under the UK's "Read-Only Data Standard," participating banks must release and make freely available both "reference information" and "product

83. The CMA9 are listed in the UK CMA Order as Barclays, HSBC, Lloyds, Nationwide, RBSG, BoI, AIB, Santander, and Danske. UK CMA Order, *supra* note 65, § 3.1.1.

84. *See Frequently Asked Questions*, BANK OF APIS, https://www.bankofapis.com/faq (last visited July 13, 2021).

85. OBIE, *Third Party Providers*, *supra* note 68.

86. OBIE, GUIDELINES FOR OPEN DATA PARTICIPANTS, *supra* note 61, at 5.

87. *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth) (Austl.) [hereinafter *CDR Banking Instrument*].

88. *Competition and Consumer (Consumer Data Right) Rules 2019* (Cth), sch 3 pt 6 (Austl.) [hereinafter *Consumer Data Rules*].

89. ACCC, CDR Timeline Update, *supra* note 73.

90. *ACCC Consultation on Proposed Timetable for Participation of Non-major ADIs in the CDR*, AUSTL. COMPETITION & CONSUMER CMM'N (Feb. 7, 2020), https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-proposed-timetable-for-participation-of-non-major-adis-in-the-cdr.

91. *Competition and Consumer Act 2010* (Cth) s 56BD(1)(b) (Austl.) [hereinafter *Competition and Consumer Act*].

92. *See generally* AUSTL. COMPETITION & CONSUMER CMM'N, DRAFT, CONSUMER DATA RIGHT SUPPLEMENTARY ACCREDITATION GUIDELINES: INFORMATION SECURITY (Sep. 23, 2019) [hereinafter ACCC, CDR SUPPLEMENTARY GUIDELINES: INFORMATION SECURITY], https://www.accc.gov.au/system/files/CDR%20draft%20supplementary%20accreditation%20guidelines%20-%20information%20security.pdf; *infra* Part III.D.

information."[93] The former includes all branch locations and opening hours, and ATM locations.[94] "Product information" covers prices, charges/interest rates, features and benefits, terms and conditions, and customer eligibility criteria for a wide range of products — including both personal and business current accounts, as well as lending products for small and medium enterprises.[95] "Service quality indicators" — results from customer surveys relating to the likelihood that they would recommend them to someone else — must also be shared.[96] The UK's framework also regulates data-sharing from a payment account[97] that is related to a specific consumer: in this type of data sharing, the bank must allow a TPP to access the data that is necessary to perform that TPP's service (excluding any data that is considered "sensitive" in that it can be used to commit fraud, e.g., personal security credentials).[98] This ensures that AISPs can access a customer's account information and transaction history,[99] while PISPs can access information regarding the initiation and execution of payment transactions.[100] Such interactions are caught by the PSD II even where they are "one leg out" (only one party is located within the EU), extending the geographical scope beyond the previous PSD (applied only to interactions taking place entirely within the EU).[101] Thus, in contrast to the CDR framework, which sometimes considers the nationality of the data subject (*see* below), the PSD II regime simply applies where one or both of the PSPs involved are located within the EU.[102]

---

93. UK CMA Order, *supra* note 65, § 10.1.

94. *Id.* § 12.1.1.

95. *Id.* § 12.1.2.

96. *Id.* §§ 13, 15.

97. *FCA Handbook: The Perimeter Guidance Manual*, 8 Fin. Conduct Auth. § 15.3 (June 2021).

98. Zunzunegui, *supra* note 59, at 17; Commission Delegated Regulation (EU) 2018/389, of 27 November 2017 Supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with Regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication, art. 36(1) 2018 O.J. (L 69) 23, 41 [hereinafter RTS].

99. RTS, *supra* note 98, art. 36(1)(a) at 41.

100. *Id.* art. 36(1)(b)–(c) at 41.

101. PSD II, *supra* note 1, art. 2(1)–(2) at 54; *Q&As: Geographical Scope of Application of the RTS on Strong Customer Authentication (SCA) and Secure Communication Requirements — Two-leg Transactions*, EUR. BANKING AUTH. (Sep. 6, 2019), https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4030; DEUTSCHE BANK, PAYMENT SERVICES DIRECTIVE 2: DIRECTIVE ON PAYMENT SERVICES IN THE INTERNAL MARKET "(EU) 2015/2366" 12 (2016) [hereinafter DEUTSCHE BANK, PAYMENT SERVICES DIRECTIVE 2], https://cib.db.com/docs_new/White_Paper_Payments_Services_Directive_2.pdf.

102. *See* DEUTSCHE BANK, PAYMENT SERVICES DIRECTIVE 2, *supra* note 101, at 12.

In Australia, "CDR data" is broadly framed under the CDR Act to include information within a class specified by a designating instrument, extending to those wholly or partly derived from such information.[103] In the banking sector, more specifically, it refers to three classes of information: "information about [a] user of [a] product" (e.g., information identifying the person), "information about use of [a] product" (e.g., information about a transaction made by the person), and "information about a product" (e.g., price, feature, and terms and conditions associated with the product).[104] CDR data can be roughly split into two categories, product data and consumer data, with only the latter specific to consumers. It is noteworthy that CDR data is qualified by geographical limitations. Generally, for data to be CDR data, it must have been generated or collected in Australia by an Australian person; or been generated or collected in Australia and related to an Australian person; or been generated or collected outside Australia by an Australian person and related to an Australian person.[105] Interestingly, access to CDR data is also currently limited to read-only privileges, contrasting to the PSD II regime's allowances for both read-only access (by AISPs) and read-write access (that is, payment initiation by PISPs).[106]

By Open Banking, the UK and Australia both extend the scope of data that is subject to access. The UK Data Protection Act 2018 features the "right to portability" as required under Article 20 of the General Data Protection Regulation ("GDPR") and makes it an offense for a controller to alter or destroy information to prevent such disclosure.[107] Although this right was set to further strengthen the control over a data subject's own data,[108] it is qualified by the fact that it applies only to "personal information" — information that relates to that identifiable person — and only that which was "provided" to the controller by the consumer.[109] By contrast, data access under the PSD II and PSR is not limited to data that is "personal" and extends beyond data provided by the consumer. As mentioned above, for instance, banks must publicly release reference/product data and service quality

103. *Competition and Consumer Act*, *supra* note 91, s 56AI (defining CDR data to include both data directly and indirectly derived from all other CDR data).

104. *CDR Banking Instrument*, *supra* note 87, ss 6–8.

105. *Competition and Consumer Act*, *supra* note 91, s 56 AC(3).

106. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, 93–94 (contrasting PSD II's requirements with CDR's).

107. Data Protection Act 2018, c. 12, § 172(3).

108. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art. 20(1), 2016 O.J. (L 119) 1, 45 [hereinafter GDPR].

109. *Id.*

indicators under the UK's additional Read-Only Standard.[110] The PSD II regime hence widens the scope of data access beyond that of the GDPR, with each approach more in line with its respective purpose. While the GDPR aims to further strengthen the control of data subjects over their own data, the PSD II also seeks to facilitate innovation and development of new Fintech services.[111]

Likewise, CDR expands the scope of data access established under Australian Privacy Principle 12 ("APP 12"). While the data access right under APP 12 is similarly qualified by "personal information,"[112] it is even more limited than its EU/UK counterpart. For instance, while the Federal Court of Australia recently in its decision of *Privacy Commissioner v Telstra Corp.*[113] interpreted the term "personal information" to have two conditions — (1) it must be "about an individual" and (2) identity is "apparent, or can reasonably be ascertained, from the information or opinion" — it offers limited guidance on when information would be considered to be "about an individual."[114] The lack of clear instructions arguably narrows the scope of application of APP 12.[115] Furthermore, APP 12 does not apply to most small businesses — those with an annual financial turnover of no more than $3 million AUD.[116] The CDR regime could address these pitfalls: it now provides access to a far greater range of information by using "consumer data" rather than "personal information" as a basis.[117]

Further, consumer data is broadly framed as covering information that is

110. UK CMA Order, *supra* note 65, §§ 12–17.

111. *See* Sophie Wijdeveld, *PSD2 Innovation and GDP Protection: A Fintech Balancing Act, Part One: Consent*, CLIFFORD CHANCE (Oct. 18, 2019), https://talkingtech.cliffordchance.com/en/data-cyber/data/psd2-innovation-and-gdpr-protection--a-fintech-balancing-act.html ("[P]ayment services providers need to balance the innovative opportunities offered by [PSD II] with the data protection challenges created by GDPR.").

112. *Privacy Act 1988* (Cth) sch 1 pt 5 s 12.1 (Austl.).

113. *Priv Comm'r v Telstra Corp* (2017) 249 FCR 24 (Austl.).

114. *Id.* at 30, 63. The Court stated that this assessment requires an "evaluative conclusion" and depends on the facts of the case. Uncertainty thus remains as to what constitutes information "about an individual" and is therefore potentially "personal information." M Feltham, *Privacy Commissioner v Telstra Corp Ltd* 14 PRIV. L. BULL. 42 (2017).

115. JAMES MEESE ET AL., CONSUMER RIGHTS TO PERSONAL DATA: DATA ACCESS IN THE COMMUNICATIONS SECTOR 28 (2019) (noting that the term "personal information" is too narrow to include all of the relevant consumer data and may result in a "confusing . . . system of data rights").

116. *Privacy Act 1988*, *supra* note 112, s 6D.

117. *See* MEESE ET AL., *supra* note 115, at 1 (calling for Australia to adopt a reform like the EU's GDPR).

"directly" or "indirectly" derived from other CDR data.[118] The latter arguably captures the data that has been re-organized, created, or otherwise value-added from "base" data. This may be worrying for industry stakeholders, as it could breach intellectual property rights,[119] reducing incentives to invest in data.[120] Consequently, information that has been "materially enhanced" is excluded from the scope of the data access rule. In the designation instrument issued for the banking industry, more specifically, "materially enhanced information" refers to data derived from product use data (source material) that has undergone "insight or analysis," which "render[s] the information significantly more valuable than the source material" by enhancing its "usefulness, usability or commercial value."[121] The exemption does not apply, however, in some circumstances — for instance, if it is publicly available, or disclosure is otherwise required by law.[122] Certain credit information like court proceeding information, personal insolvency, or serious credit infringement is explicitly excluded from the scope of disclosure.[123]

While significant expansions to the scope of data access have thus been made, there are plans in both nations to extend this even further. The UK's Smart Data Initiative will apply similar data sharing across the "regulated markets" (e.g., utilities, communications, rail, and financial services)[124] and

118. *Competition and Consumer Act*, *supra* note 91, s 56AI (1)–(2).

119. In the context of EU/UK, in particular, this can also turn on the clash between the Open Banking initiative and the *sui generis* "database right" contained in article 7(1) of Directive 96/9/EC, of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases 1996 O.J. (L 77) 20; transposed by regulations 13 and 14 of The Copyright and Rights in Databases Regulations 1997, SI 1997/3032. No such right exists in Australia, where databases may only be protected if they fall under general copyright law. *See IceTV Pty Ltd v Nine Network Australia Pty Ltd* (2009) 239 CLR 458.

120. *See* THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 36–38 (arguing that obliging data holders to share their "value-added" data may in fact have negative impacts on investment, intellectual property, and commercial agreements and recommending that this type of data not be included within Open Banking).

121. *CDR Banking Instrument*, *supra* note 87, s 10(1). To set a clear standard, section 10(3) lists information that is "not materially enhanced information," including, notably, calculated balances, amount of interest earned or charged, and fees charged, among others.

122. *Id.* s 10(2).

123. *Id.* s 9.

124. *See* Dep't for Digit., Culture, Media & Sport, *National Data Strategy*, U.K. GOV'T, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy (last updated Dec. 9, 2020); *see also* HM GOV'T (U.K.), NEXT STEPS FOR SMART DATA: PUTTING CONSUMERS AND SMES IN CONTROL OF THEIR DATA AND ENABLING INNOVATION 13 (2020) [hereinafter HM GOV'T (U.K.), NEXT STEPS FOR SMART DATA].

possibly the "digital market" (e.g., social media companies).[125] While Australia intends to apply its Consumer Data Right to the energy and telecommunications sectors before eventual "economy-wide" implementation.[126]

C. Who Should Bear Losses Caused?

Open Banking brings both benefits and risks. While data can be held and used by more entities, this also entails more points of storage and stages in which data could be compromised.[127] Unauthorized[128] or defective[129] transactions therefore lead to issues of liability: which party bears the loss resulting from fraudulent or erroneous activities?[130] Previously, where consumers shared their banking login credentials with data aggregators via screen scraping, they were often responsible for losses arising from unauthorized transactions.[131] Such an issue becomes more problematic with

125. *See* HM GOV'T, NEXT STEPS FOR SMART DATA, *supra* note 124, at 17.

126. Explanatory Memorandum, CDR Bill, *supra* note 71, at 5, 7–8 (outlining the stages of implementation).

127. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 50 (noting that more points of storage make it easier for the data to be hacked and more transfers increase the risk that the data may be sent to the incorrect user); *Trust in Open Banking: Negotiating Data Liability Between Banks and TPPs*, FINEXTRA (Nov. 22, 2019) [hereinafter, FINEXTRA, *Trust in Open Banking*], https://www.finextra.com/newsarticle/34820/trust-in-open-banking-negotiating-data-liability-between-banks-and-tpps (acknowledging the need to address "the threat of losing [data and ensuring it] remains the central priority").

128. An "unauthorized transaction" is a transaction made without the customer's consent. *See, e.g.*, PSD II, *supra* note 1, art. 64(1) at 91 ("[A] payment transaction is considered to be authori[z]ed only if the payer has given consent to execute the payment transaction.").

129. A "defective transaction" is a transaction "requested by the customer but wrongly processed by the providers involved" (which may incur charges from the intended recipient). INST. OF INT'L FIN., LIABILITY AND CONSUMER PROTECTION IN OPEN BANKING 1 (2018), https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf.

130. *See* BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 14 (stating regulatory frameworks and approaches to the issue of liability for data breaches); Reinhard Steennot, *Reduced Payer's Liability for Unauthorised Payment Transactions Under the Second Payment Services Directive (PSD2)* 34(4) COMP. L & SEC. REV. 954, 957 (2018) (exploring liability issues arising from data sharing); INST. OF INT'L FIN., *supra* note 129, at 5 (noting that in countries like the United States, with no specific regulatory framework for such liability issues, bilateral agreements will sometimes dictate liability, otherwise the customer may have to resort to a civil suit).

131. *See* BASEL COMM., REPORT ON OPEN BANKING, *supra* note 7, at 14 (noting that in the absence of a clear framework, when "customer-permissioned data" falls into the hands of the wrong party, it is difficult to determine how much responsibility should fall on the customer).

multiple entities involved in the provision of services in the Open Banking context: consumers, banks, TPPs and even fourth parties.[132]

Jurisdictions following the mandatory approach, such as the EU/UK, have a dedicated framework to address these issues.[133] Presumably, such rules may overcome several challenges seen in jurisdictions with no specific regulatory intervention — a consumer in the United States, for example, may hope for a bilateral agreement between their banks and the third party for dispute resolution, but in its absence, must rely solely on the civil liability framework.[134] Consumers under the latter system typically have to assume the burden of proof by identifying which party may have made a mistake to hold it accountable.[135] The EU/UK liability regime, in contrast, reverses the default setting by shifting the burden to service providers in several ways and requiring that consumers receive a refund for their loss except in limited circumstances (as discussed below).[136]

Likewise, in Australia, such allocation of responsibility was considered "important for the proper functioning of Open Banking,"[137] as clarifying the liability for each party would "build community trust and confidence."[138] It would also offer certainty for industry participants like data holders and data recipients, and eliminate bilateral negotiations surrounding the liability risks associated with Open Banking — although such a regime has not yet been put in place in Australia.[139] The Australian Treasury's *Review into Open Banking* contrasted this to market-driven attribution of liability, which could result in less-informed parties accepting the associated risks as "buried in a dense set of terms and conditions and therefore not readily understood and

132. *Id.* at 7, 14 (explaining that as more parties gain access to and share data, identifying and assigning liability in the case of erroneously shared data becomes more difficult).

133. *See* INST. OF INT'L FIN., *supra* note 129, at 3 (exemplifying the PSD II and its guidelines as a regulation that provides rules on "liability conditions").

134. *Id.* at 5.

135. *Id.* (calling out the "worst-case scenario," in which case the information necessary to meet this burden of proof is often "outside the consumer's reach" and noting that even once this burden is met, the consumer must carry litigation's additional burdens of time and expense).

136. *Id.* (explaining, for instance, that the EU requires professional indemnity insurance, or its equivalent, for third parties accessing consumer account information and that the bank must refund the consumer before requesting compensation from liable third parties).

137. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 65.

138. *Id.*

139. *Id.* (emphasizing the importance of "consistency and transparency across all data sharing arrangements . . . [to] provide certainty for customers on who bears the liability for any losses").

genuinely agreed to."[140] Against this backdrop, we now turn to the substance of such frameworks in the EU/UK and Australia.

i. EU/UK Model

In the UK, the liability framework is set forth under its Payment Services Regulations 2017 ("PSR 2017"),[141] which transposed the EU's PSD II.[142] Overall, PSR 2017 uses a rule of thumb whereby banks — termed Account Servicing Payment Service Providers ("ASPSP") — must immediately reimburse the customer for the loss caused by an unauthorized transaction, regardless of whether it occurred as a result of third-party access.[143] This does not apply where the bank "has reasonable grounds to suspect fraudulent behavior" by the customer and fulfills the relevant notification obligation.[144] Furthermore, per PSR 2017, if there is a deficiency when executing a payment transaction (e.g., non-execution, late execution, incorrect execution) and such payment was initiated through a TPP — specifically, a PISP — it is the bank that will be liable.[145] However, if the PISP is found to be responsible for the unauthorized or deficiently executed transaction, it must then compensate the bank.[146] As a general rule, the burden will fall on either the bank or TPP to show that the transaction was authenticated rather than on customers to prove otherwise.[147] Furthermore, both PISPs and AISPs must have professional indemnity insurance (or a comparable guarantee).[148]

The EU/UK regime articulates a set of interrelated obligations governing the customers, banks, and TPPs concerning liability. Customers, termed "payers" under PSR 2017, are obliged to notify their bank when they learn an unauthorized transaction has taken place and wish to seek rectification.[149] They must make such a notification "without undue delay" on becoming aware of the transaction, and "in any event, no later than 13 months after the

140. *Id.*

141. Payment Services Regulations 2017, SI 2014/752 [hereinafter PSR].

142. Payment Services Regulations 2017 Explanatory Memorandum, c. 2, Explanatory Notes ¶ 1.

143. PSD II, *supra* note 1, art. 73 at 96; PSR, *supra* note 141, art. 76; FINEXTRA, *Trust in Open Banking*, *supra* note 127.

144. PSR, *supra* note 141, art. 76, ¶ 3.

145. PSD II, *supra* note 1, art. 73(2) at 96; PSR, *supra* note 141, art. 76, ¶ 5(a).

146. PSD II, *supra* note 1, art. 73(2) at 96; PSR, *supra* note 141, art. 76, ¶ 5(b), art. 95.

147. *See, e.g.*, PSR, *supra* note 141, art. 75.

148. PSD II, *supra* note 1, art. 5(2)–(3) at 62; PSR, *supra* note 141, art. 6, ¶ 7(e)–(f).

149. PSD II, *supra* note 1, art. 71(1) at 96–97; PSR, *supra* note 141, art. 74, ¶ 1.

debit date."[150] A logical consequence following customers' failure to do so would be — though not expressly spelled out in the regime — that they bear all losses arising from unauthorized transactions (i.e., they lose their statutory entitlement reimbursed by the bank).[151] Further, it is less clear whether a customer can get their account rectified if he or she has "undue delay" — a term left undefined — in making such notification within the prescribed 13 month timeframe.[152]

Relatedly, while it is not clear whether a customer should also contact the TPP, the foregoing notification duty will, as a matter of practice, effectively make the bank the first contact.[153] Questions continue to go unanswered: should the bank then pass this information onto the TPP for investigation upon receiving a notification from customers? What can and should be done by the bank while the TPP investigates the unauthorized transaction? Although the PSR 2017 appears silent on these issues, the FCA has stated that the bank and TPP are permitted to have voluntary arrangements to settle such liabilities.[154]

A more difficult question arises if both the bank and TPP deny any wrongdoing after the notification. While it is clear here that customers would not be caught in the middle — they will be reimbursed by the bank anyway, no matter who would be ultimately liable — it is less obvious as to the allocation of burden of proof between banks and TPPs. The FCA has clarified, in terms of payments initiated via a TPP, that the burden "lies with

150. PSR, *supra* note 141, art. 74, ¶ 1; *see* PSD II, *supra* note 1, art. 71(1) at 96–97.

151. However, this issue is not entirely clear and there has been no specific guidance from the EU nor from the FCA. Kai Zhang, *Payer Liability under PSD2 — Unintended Complexity?* BRYAN CAVE LEIGHTON PAISNER (June 27, 2019), https://www.bclplaw.com/en-US/thought-leadership/payer-liability-under-psd2-unintended-complexity.html (reasoning that this allocation of liability encourages customers to timely report any unauthorized payment transaction).

152. Steennot, *supra* note 130, at 116 (observing that "it remains unclear whether the payer can still obtain rectification if he [was] notified [of] the unauthorized transaction within 13 months, but not without undue delay after becoming aware of the unauthorized transaction").

153. *See Open Banking, Open Liability: Accountability Issues for Open Banking APIs*, ASHURST (Feb. 28, 2018) [hereinafter *Open Banking, Open Liability*], https://www.ashurst.com/en/news-and-insights/legal-updates/open-banking-open-liability-accountability-issues-for-open-banking-apis/ (questioning whether it is the best practice for banks to serve as the refund point of contact, especially "where there is a direct interaction between TPP and the customer").

154. FIN. CONDUCT AUTH., PAYMENT SERVICES AND ELECTRONIC MONEY — OUR APPROACH. THE FCA'S ROLE UNDER THE PAYMENT SERVICES REGULATIONS 2017 AND THE ELECTRONIC MONEY REGULATIONS 2011 122, 139 (2019) [hereinafter FCA APPROACH DOCUMENT], https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

the PISP to show that it was not responsible for the error."[155] The PISP thus needs to show that the payment order was correctly handled within its "sphere of influence" — that is, the parts of the transaction over which the PISP has control.[156] Nevertheless, what would trigger this "sphere of influence" expression remains unclear in practice.[157]

If, on the other hand, the loss or misappropriation of the payment instrument was traced to the customer, that customer would be liable for losses up to a maximum of £35.[158] Yet, customers would assume full liability for losses — without a cap — if they have acted fraudulently, or otherwise intentionally, or with gross negligence breached the obligations[159] concerning the use of the payment instrument[160] and the safe-keeping of security credentials.[161] Some intriguing issues emerge from this context. First, what yardsticks are used to assess "detectability"? Second, how is the notion of "gross negligence" interpreted in this context? On the former, PSR 2017 and PSD II are largely silent, thus leaving room for debate in practice.[162] On the latter, PSD II in its recitals makes clear that "gross negligence" must be more than a mere breach of a duty of care; rather, it refers to conduct that exhibits "a significant degree of carelessness."[163] Prime examples include writing a PIN on a note that is kept besides the payment instrument, leaving the payment instrument in an easily accessible place, or typing in a password knowing that a person is watching.[164] The

155. *Id.* at 139.

156. *Id.* ("[The PISP must show] that the payment order was received by the customer's ASPSP and, within the PISP's sphere of influence, the payment transaction was authenticated, accurately recorded[,] and not affected by a technical breakdown or other deficiency.").

157. *Open Banking, Open Liability*, *supra* note 153 (noting that the "sphere of influence" may still lead to disputes).

158. PSD II, *supra* note 1, art. 74(1) at 96–97; PSR, *supra* note 141, art. 77, ¶¶ 1–2. Note that under the PSD II, this limit is €50. However, the customer will not be liable for any amount where the loss was not detectable, or where the loss was caused by an employee, agent, or branch of a PSP, or its outsourced provider.

159. These obligations are imposed under PSD II Articles 69 and 74. PSD II, *supra* note 1, art. 69, 74 at 94, 96–97; PSR, *supra* note 141, art. 72.

160. According to the FCA, "'payment instrument' has a wide definition . . . includ[ing] payment cards, e-banking[,] and telephone banking arrangements." FCA APPROACH DOCUMENT, *supra* note 154, at 98.

161. PSD II, *supra* note 1, art. 74(1) at 96–97; PSR, *supra* note 141, art. 77, ¶ 3.

162. "Detectable" is not defined in PSD II Article 4 ("Definitions"), nor in Article 74 ("Payer's liability for unauthorised payment transactions"). *See also* Zhang, *supra* note 151 (identifying PSR provisions where the meanings of certain threshold words are ambiguous).

163. PSD II, *supra* note 1, recital 72 at 47.

164. *Id.*; Steennot, *supra* note 130, at 961.

FCA clarified that "it is not sufficient . . . to assert that the customer 'must have' divulged" security credentials[165] — further underscoring that evidence must be provided to prove fraud or gross negligence, with the burden of proof once again on the bank.[166]

It comes as no surprise that allocation of liability has been one of the most controversial issues under the PSD II regime.[167] Banks are the first port of call for refunds even where there is a direct interaction between a customer and TPP, with banks citing this liability model to be a "key challenge" of third-party access.[168] The Institute of International Finance has recommended that responsibility should instead lie first on the party (the bank or TPP) from which the transaction originated.[169]

In brief, notwithstanding some ambiguities around the liability allocation arrangements, the current regime under the PSD II/PSR 2017 has been working towards being more payer (customer)-friendly than its predecessor.[170] Customers can, for instance, have the same protection if they use a PISP to initiate the transactions.[171] Customers' liability for losses not arising from grossly negligent or intentional breach of their obligations has been reduced from £50 to £35.[172] Furthermore, supporting evidence is required to prove a customer's fraud or gross negligence, and gross negligence has been clarified to require more than a mere breach of the duty of care.[173] Some commentators thus point out that under the new regime, "if one actually keeps his personalized security credentials safe, risks [for the customer] become very limited."[174]

---

165. FCA APPROACH DOCUMENT, *supra* note 154, at 123–24.

166. PSD II, *supra* note 1, art. 72(2) at 96; PSR, *supra* note 141, art. 75, ¶ 4.

167. *See Open Banking, Open Liability*, *supra* note 153 (emphasizing that the European Payments Council expressed discontent with banks being held liable when they already take on financial risks and burdens).

168. *See* DELOITTE, EUROPEAN PSD2 SURVEY: VOICE OF THE BANKS 10 (2018), https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte_European_PSD2_Voice_of_the_Banks_Survey_012018.pdf (listing primary challenges that banks identified with the PSD II).

169. INST. OF INT'L FIN., *supra* note 129, at 6.

170. *See* Steennot, *supra* note 130, at 963 (listing ways in which the PSD II regime increases customer protections).

171. PSD II, *supra* note 1, art. 73(2) at 96; PSR, *supra* note 141, art. 76, ¶ 5; Steennot, *supra* note 129, at 963.

172. Payment Services Regulations 2009, SI 2009/209, art. 62, ¶ 1, which set a maximum of £50 for such payer's liability, has been replaced by PSR 2017, art. 77, ¶ 1, which sets a maximum of £35.

173. PSD II, *supra* note 1, art. 72(2) at 96; PSR, *supra* note 141, art. 75, ¶ 4; Steennot, *supra* note 129, at 963–64.

174. Steennot, *supra* note 129, at 964.

Allocating liabilities raises two inter-related questions. One, what can be done about the fact that unauthorized transactions could go hand in hand with the lack of security measures? Two, what, if any, mechanism is put in place to address disputes arising from the Open Banking context? On the former, the EU/UK framework requires "strong customer authentication" and places rather strict liability on banks — no liability can be imposed on customers in the absence of such mechanisms.[175] As for the latter, the UK's Open Banking Standard has gone beyond PSD II to establish a Dispute Management System ("DMS").[176] Although it does not offer a liability or dispute resolution model in itself, it creates common best practice principles for banks and TPPs.[177]

ii. Australian Model

As in the UK, an accredited data recipient must have adequate insurance (or comparable guarantee) to compensate consumers for losses arising from contravention of duties under the CDR regime.[178] They may, subject to the services they offer and potential liability exposure, require professional indemnity insurance, cyber insurance, or both.[179]

A CDR participant is protected from liability under Section 56GC of the CDR Act where they provide CDR data as per the regulations and Consumer Data Rules. Unlike the PSD II/PSR 2017, however, the CDR does not contain a liability framework itself. Thus, the "ePayments Code" — to which most banks subscribe — would appear the most relevant instrument that comes into play concerning liabilities associated with unauthorized transactions. There are issues around the use of the ePayments Code in this context. First, the ePayments Code is voluntary and does not apply to TPPs unless they subscribe to it.[180] Second, while the ePayments Code has one chapter dedicated to allocating liability arising from unauthorized

175. PSD II, *supra* note 1, art. 74(2) at 97; PSR, *supra* note 141, art. 77, ¶ 4(c); *see infra* Section III.D.

176. *See Dispute Management System*, OBIE, https://www.openbanking.org.uk/providers/dispute-management-system/ (last visited July 13, 2021).

177. INST. OF INT'L FIN., *supra* note 129, at 5 ("The DMS is a voluntary mechanism under which participants adhere to a code of best practices, including on how to handle cases at the first instance, and how those can be taken to mediation, adjudication or arbitration.").

178. *Consumer Data Rules*, *supra* note 88, r 5.12(2)(b).

179. AUSTL. COMPETITION & CONSUMER CMM'N, DRAFT, CONSUMER DATA RIGHT SUPPLEMENTARY ACCREDITATION GUIDELINES: INSURANCE 5 (Sep. 23, 2019), https://www.accc.gov.au/system/files/CDR%20draft%20supplementary%20accreditation%20guidelines%20-%20insurance.pdf.

180. AUSTL. SEC. & INV. COMM'N, EPAYMENTS CODE 2 (2016), https://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf.

transactions, its focus is on the relationship between subscribing banks and customers.[181] More specifically, the ePayments Code provides a set of rules under which a customer (i.e., account-holder) will only be liable for losses in specified circumstances: for instance, where the customer contributed to the loss by "unreasonably delaying reporting the misuse, loss, or theft of a device" or breach of passcodes,[182] or where the bank can prove "on the balance of probabilities that [the customer] contributed to a loss through fraud or breaching the passcode security requirements."[183] Notably, a breach of the passcode security requirement could cover acts like voluntary disclosure of a customer's login credentials to a third party, or recording passcodes on anything carried with the device, or otherwise "act[ing] with extreme carelessness in failing to protect the security" of passcodes.[184] In such cases, the customer may be liable for any losses arising from associated unauthorized transactions.[185] Therefore, the ePayments Code may struggle to accommodate screen scraping practices as customers are likely to breach the security requirement if they share data with TPPs.[186] The legality of screen scraping technologies with the ePayment Code has become a source of debate, which will be considered later.[187] In summary, unlike its EU/UK counterpart, the CDR has not yet articulated a full-fledged regime allocating the liabilities between different parties in the contemporary Open Banking ecosystem.

D. How to Address Security and Privacy Concerns?

Although the risks associated with data sharing are not entirely novel, the greater access to data does increase the potential points of cyber-attacks and

181. *See generally id.* (noting that the Code regulates electronic payment services and "banks, credit unions, building societies and other providers of electronic payment facilities to consumers subscribe").

182. *Id.* s 11.5.

183. *Id.* s 11.2.

184. *Id.* s 12.

185. *Id.* s 11.

186. *See* THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 51 (recognizing that the ASIC has not formed a definitive view on screen scraping, though quoting the ASIC's belief that "such actions could be viewed as the consumer breaching the standard banking terms and conditions for non-disclosure of passwords . . . in the ePayments Code"); *see also ASIC & ACCC: Screen Scraping is a Valid Method of Data Sharing*, AUSTL. FINTECH (Mar. 9, 2020), https://australianfintech.com.au/asic-accc-screen-scraping-is-a-valid-method-of-data-sharing-2/; James Eyers, *ASIC, ACCC Give Green Light to 'Screen Scraping'*, FIN. REV. (Feb. 28, 2020), https://www.afr.com/companies/financial-services/asic-accc-give-green-light-to-screen-scraping-20200228-p54588.

187. *See infra* Part III.E.

data breaches.[188] How to manage these concerns has become a daunting task for policymakers in both the UK and Australia, as discussed below.

i. EU/UK Model

The PSD II states that it "guarantees a high level of consumer protection, security of payment transactions, and protection against fraud."[189] It also stresses that the national authorities should "have in place adequate and effective safeguards" to respect fundamental rights, including privacy.[190] To this end, it sets out various mechanisms — from rigorous authentication methods to mandatory risk management and reporting systems. However, it has been debated whether these measures are resilient enough in managing security and data protection concerns.[191]

Regarding security concerns, the EU/UK regime allows banks to deny TPPs access to a payment account for "objectively justified and duly evidenced reasons relating to unauthori[z]ed or fraudulent access to the payment account."[192] In such cases, the bank shall inform the customer "before access is denied and at the latest immediately thereafter."[193] Also, banks must report such incidents to the relevant authority (in the UK, the FCA).[194]

More generally, all PSPs under the PSD II/PSR 2017 are required to have a framework with appropriate measures and control mechanisms to manage operational and security risks.[195] Such a framework should be "proportionate to its size and the nature, scope, complexity and riskiness of its operating

188. Pieter T.J. Wolters & Bart P.F. Jacobs, *The Security of Access to Accounts Under the PSD2*, 35 COMP. L. & SEC. REV. 29, 30 (2019) (arguing that customers within an open banking system are vulnerable at more points to their information being abused for "identity theft, blackmail, [or] illegal pricing discrimination").

189. *Id.* at 30; *see* PSD II, *supra* note 1, recitals 5–7, 33, 42, 66–67, 69, 75, 77, 84–85, 95, 109 at 36, 40, 42, 46–49, 51, 53.

190. PSD II, *supra* note 1, recital 46 at 42.

191. *See, e.g.*, Wolters & Jacobs, *supra* note 188, at 40–41 (arguing that these measures, like robust authentication, are inadequate and are subordinate to the goal of market development).

192. PSD II, *supra* note 1, art. 68(5) at 94; PSR, *supra* note 141, art. 71, ¶ 7.

193. PSD II, *supra* note 1, art. 68(5) at 94; PSR, *supra* note 141, art. 71, ¶ 8(a)–(b).

194. PSD II, *supra* note 1, art. 68(6) at 94; PSR, *supra* note 141, art. 71, ¶ 8(c).

195. These obligations apply to not only banks but to AISPs and PISPs, which must become an authorized provider to access data under PSD II. Such authorization will only be granted if the relevant national authority is satisfied that the company is suitable to provide AIS or PIS based on their internal control mechanisms (i.e., systems safeguarding the business from fraud and error), risk management procedures (e.g., risk identification, monitoring, and customer authentication), and incident response (e.g., monitoring and reporting policies), among others. PSD II, *supra* note 1, arts. 5, 95–96 at 59–63, 104–05; PSR, *supra* note 141, arts. 5, 98–99, sch. 2.

model, and of the payment services it offers."[196] A PSP is required to notify the FCA without undue delay in the event of a noteworthy operational or security breach.[197] Another notable design is the introduction of the "strong customer authentication" ("SCA") requirement. Where customers wish to use services offered by a TPP, SCA requirements would generally apply.[198] SCA involves a customer's demonstration of at least two of three types of identity verification: knowledge (e.g., a password), possession (e.g., possessing a particular mobile device by accepting a push notification), and/or inherence (e.g., fingerprint or iris recognition).[199] While SCA must be used in all other cases,[200] there are certain exemptions based on payment avenue, frequency, degree of risk, and amount of the transaction[201] — a provider can, for instance, choose not to apply SCA in transactions involving low amount, [202] low risk, [203] or "trusted beneficiaries" nominated by the customer. [204] These exemptions attempt to balance security and payment interests.[205] Notably, a bank forgoing SCA under an exemption will alter the allocation of liability (to its detriment) in regard to losses from unauthorized transactions. While a customer would usually be liable if they acted with "gross negligence" in failing to keep payment instruments or credentials safe,[206] in circumstances where SCA is not used by the bank, the customer will instead only bear losses where they have acted *fraudulently*.[207] Overall, the SCA method increases the certainty that the legitimate customer wishes to make a payment or access their account, rather than someone attempting to commit fraud.[208]

All firms that wish to participate in the Open Banking regime must be subject to common standards for communication, authentication, data

196. FCA APPROACH DOCUMENT, *supra* note 154, at 242.

197. PSD II, *supra* note 1, art. 96(1) at 105; PSR, *supra* note 141, art. 99, ¶ 1.

198. PSD II, *supra* note 1, art. 97 at 106; PSR, *supra* note 141, art. 100. It is the TPP that is obliged to apply the SCA, while the bank must simply allow the TPP to rely on the authentication procedures provided to the customer.

199. PSD II, *supra* note 1, art. 4(30) at 59.

200. *Id.* art. 97 at 106; PSR, *supra* note 141, art. 100.

201. PSD II, *supra* note 1, art. 98(3) at 107; FCA APPROACH DOCUMENT, *supra* note 154, at 256. The exemptions are transposed into UK law by PSR art. 100, ¶ 5.

202. RTS, *supra* note 98, art. 16 at 32.

203. *Id.* art. 18 at 33.

204. Such exemptions are specified in the RTS. *Id.* arts. 10–18 at 31–33.

205. Zunzunegui, *supra* note 59, at 29–30.

206. PSD II, *supra* note 1, art. 74(1) at 96.

207. *Id.* art. 74(2) at 97.

208. *See* RTS, *supra* note 98, art. 2 at 28–30.

storage, and security.[209] Many of these requirements are set forth under the Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication ("RTS"). The RTS took effect in 2019 after being released by the European Banking Authority ("EBA") in cooperation with the European Central Bank ("ECB") and was then approved as a Commission delegated regulation.[210]

The RTS elaborates on managing operational and security risks under the PSD II, which has been adopted in the UK.[211] For instance, both banks and TPPs are required by PSD II/PSR 2017 to ensure that they communicate with each other "in a secure way" and per the specific standards set out by the RTS.[212] To this end, the RTS fleshes out detailed requirements for secure communication like the use of "strong and widely" recognized encryption techniques,[213] keeping sessions as short as possible, [214] limiting staff access to confidential information,[215] and various obligations for interfaces.[216] It also requires "transaction monitoring mechanisms" to be in place to detect unauthorized or fraudulent transactions.[217]

These RTS requirements are elaborated upon in the UK's data standards, released by the OBIE.[218] This is an independent, private entity funded and organized mainly by the CMA9 banks,[219] although some public oversight mechanisms are in place.[220] The decision-making body of OBIE consists of

209. *See generally* THE OPEN BANKING STANDARD, OPEN DATA INSTITUTE (Louise Bolotin ed. 2020), http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf (explaining that with Open Banking, financial institutions must adopt uniform standards across the industry).

210. RTS, *supra* note 98, art. 38(2) at 42.

211. For example, the security measures referred to in regulations 68, 69, 70, 77, and 100 of the PSR are adopted from the RTS. FCA APPROACH DOCUMENT, *supra* note 154, at 211.

212. PSD II, *supra* note 1, arts. 66(3)(d), 67(2)(c) at 92–93.

213. RTS, *supra* note 98, art. 35(1) at 41.

214. *Id.* art. 35(2) at 41.

215. *Id.* art. 35(5) at 41.

216. *Id.* arts. 30–33 at 37–40.

217. *Id.* art. 2(1) at 27–28.

218. *Read-Write Data API Specifications*, OBIE, https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1077805207/Read+Write+Data+API+Specification+-+v3.1.2 (last updated Aug. 20, 2019).

219. COMPETITION & MKTS. AUTH., RETAIL BANKING MARKET INVESTIGATION 441 (2016) (ordering the UK's nine largest banks to set up an Implementation Entity "tasked with agreeing, implementing, and maintaining open and common banking standards").

220. The chair is accountable to the CMA and must provide monthly reports to them. The steering group includes observers from four public bodies (the HM's Treasury, the FCA, the Payment Systems Regulator, and the Information Commissioner's Office). *See id.* at 39; UK CMA Order, *supra* note 65, sch. 1 item 2.

CMA9 representatives, customer representatives, and representatives from various stakeholder groups (e.g., Fintechs).[221] These parties collectively shape the data standards released by OBIE, imposing various requirements (such as API, data format, and security standards) that ensure the practical and secure functioning of Open Banking.[222] Besides security measures, the EU/UK regime is also concerned with a potential data breach by stating at the outset that "data protection by design and data protection by default should be embedded in all data processing systems"[223] and that personal data should be provided and processed "in accordance with Directive 95/46" — the predecessor of the GDPR.[224] As for the interaction between the GDPR and the PSD II, several points are noteworthy. First, it is generally agreed that the PSD II is not "*lex specialis*" vis-à-vis the GDPR, but rather provides a specific framework on how payment data should be accessed.[225] The European Data Protection Board ("EDPB"), for instance, in its response to the Dutch Data Protection Authority, implied as much about Article 94 of the PSD II by stating that, "the interpretation and the implementation of the articles in PSD2 have to be made in light of the GDPR."[226] BEUC — the European Consumer Organisation — made this point even clearer:

> *[A]ccess to bank account information can very often reveal sensitive data which would fall under Article 9 GDPR.* Explicit consent under the GDPR should be required as the legal basis for processing in those situations where special categories of data would be involved. Otherwise, banks and

221. UK CMA Order, *supra* note 65, sch. 1 Part A. Specifically, stakeholder views are presented by the conveners of advisory groups (representing Fintechs, challenger banks, PSPs, and others).

222. *Id.* § 10.1 (detailing providers' requirements to implement and maintain "without charge" open API and data sharing standards).

223. PSD II, *supra* note 1, recital 89 at 50.

224. *Id.* art. 94(1) at 104. Article 94 of the GDPR states that references to the repealed Directive shall be read as references to GDPR.

225. *See, e.g.*, EUR. BANKING FED'N, GUIDANCE FOR IMPLEMENTATION OF THE REVISED PAYMENT SERVICES DIRECTIVE 83 (2019) [hereinafter EBF, PSD2 GUIDANCE], https://www.ebf.eu/wp-content/uploads/2020/01/EBF-PSD2-Guidance-Final-v.120.pdf; FCA APPROACH DOCUMENT, *supra* note 154, at 220 ("A PSP must ensure that it meets its obligations under both the PSRs 2017 and data protection law cumulatively."); *cf.* Giangiacomo Olivi, *PSD2: Legal Issues in Open Banking (and GDPR!)*, DENTONS (Feb. 26, 2019), https://www.dentons.com/en/insights/articles/2019/february/26/psd2-legal-issues-in-open-banking-and-gdpr (explaining that PSD II "could be *lex specialis* with respect to GDPR" because the PSD II passed in 2015, before the GDPR was enacted).

226. Letter from Andrea Jelinek, Chairperson, Eur. Data Prot. Bd., to Sophie in 't Veld, Member, Eur. Parliament 2 (July 5, 2018) [hereinafter EDPB 2018 Letter], https://edpb.europa.eu/sites/edpb/files/files/file1/psd2_letter_en.pdf (explaining that GDPR data protections must be consistently applied throughout the EU because, under Article 94, "references to the repealed Directive 95/46 shall be construed as references to the GDPR").

> TPPs would be actively circumventing the GDPR. In this sense, PSD II is not *lex specialis*.[227]

Two related issues arise from the above observation. For one, each Open Banking participant should be considered as a separate data controller and should be responsible for its own data processing. While banks are obliged to ensure data access by TPPs via dedicated interfaces, such third parties are not selected by banks; thus, banks do not have the duty to ascertain a TPP's GDPR compliance.[228]

For another, the term "consent" should be read differently under the PSD II and the GDPR — they have different functions with different requirements. Specifically, data sharing under Article 94(2) of the PSD II and Regulation 97 of the PSR 2017 is conditioned upon a customer's "explicit consent," which is an "additional requirement of a contractual nature" and is "not the same as (explicit) consent under the GDPR."[229] The consent in the Open Banking regime should be understood therefore in conjunction with GDPR Article 6(1)(b) given that processing data is necessary for the performance of a contract to which the data subject is a party. Accordingly, "when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree[] to these clauses."[230] For purposes other than those necessary for performing a contract, one can rely on "consent" under GDPR Article 6(1)(a), provided that other conditions are met.[231] In short, PSD II increases the standard of data protection by imposing additional consent.

Another sticking issue around consent arises when a consumer allows a TPP access to their data, such data would often involve the transactions

---

227. EUR. CONSUMER ORG. (BEUC), BUEC'S RECOMMENDATIONS TO THE EDPB ON THE INTERPLAY BETWEEN THE GDPR AND PSD2, 3–4 (2019), https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf.

228. *See* EBF, PSD2 GUIDANCE, *supra* note 225, at 84.

229. EDPB 2018 Letter, *supra* note 226, at 4 ("Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.").

230. *Id.*

231. Specifically, those conditions set forth under Articles 4(11) and 7 of the GDPR. Some practitioners suggest that, from a practical perspective, PSPs will have to "build an explicit consent mechanism aligned with the PSD2, but not with the GDPR. As far as GDPR is concerned, they will have to rely on another lawful basis (namely, contractual necessity) to process data from a GDPR perspective." Scott McInnes et al., *EU: The Interplay of PSD2 and GDPR — Some Select Issues*, BIRD & BIRD (Feb. 2019), https://www.twobirds.com/en/news/articles/2019/global/eu-the-interplay-of-psd2-and-gdpr-some-select-issues.

between that customer with a third party — the so-called "silent party."[232] Would processing a silent party's data put TPPs inconsistent with the GDPR absent the consent of that such party? In this regard, the EDPB stated that in the case of TPPs, the "legitimate interests pursued by the controller or by a third party" under GDPR Article 6(1)(f) should provide a lawful basis for processing a silent party's personal data.[233] Yet, the EDPB noted that this legitimate interest must not be "overridden by the interests or fundamental rights and freedoms of the data subject," and such processing must be unavoidable, comparable, and align with other GDPR principles like "purpose limitation, data minimi[z]ation and transparency."[234]

Speaking of data minimization, the PSD II regime does mirror what is required under GDPR Article 5(1)(c). For instance, in the context of AISP PSD II only allows entities to request and access the information that is necessary to initiate the payment transaction.[235] Relatedly, the PSD II excludes "sensitive payment data" (e.g., personalized security credentials) from the scope of the access to accounts.[236]

Notwithstanding these security and data protection measures, there are still concerns. In terms of security measures, notably, there are criticisms against the "fall-back" option allowing the use of screen scraping.[237] It is also argued that the PSPs have considerable discretion to organize the authentication process, which can undermine the goal to make the process as secure as possible.[238] It is likewise suggested that the data minimization principle could be easily compromised by TPPs by offering a wide range of services.[239] However, these pitfalls do not necessarily mean that customers lack adequate protection as a matter of practice: it remains to be seen how

232. For instance, a customer named John transferred money to his friend Jane to share dining costs. If John decides to use an AISP's services by allowing the bank to share data, Jane's information would be included as part of that information. *See* EDPB 2018 Letter, *supra* note 226, at 2.

233. *See id.* at 3.

234. *Id.*

235. *See, e.g.*, PSD II, *supra* note 1, arts. 66(3)(f), 66(3)(g), 67(2)(d) at 92–93; PSR, *supra* note 141, art. 69, ¶ 3(f), art. 70, ¶ 3(d).

236. PSD II, *supra* note 1, arts. 4(32), 67(2)(e), at 59, 93; PSR, *supra* note 141, art. 2, ¶ 1, art. 70, ¶ 3(e).

237. *See infra* Part III.E.

238. Wolters & Jacobs, *supra* note 188, at 29 (noting that "banks do not seem required to trust this process" and banks do not need to be able "to verify the authentication or the integrity of the payment order").

239. *Id.* at 32 (stating that the required information "depends on the offered service;" therefore, if a broad range of services are offered, the limitation can be avoided).

the security and data protection requirements will be tested in the next few years.[240]

ii. Australia Model

According to the Australian Information Commissioner, "securing CDR data is an integral element of the CDR regime."[241] Like in its EU/UK counterpart, authorization is an effective tool: data relating to identifiable consumers can generally only be transferred to Accredited Data Recipients ("ADR") (or the consumer themselves).[242] To become accredited,[243] a TPP must demonstrate sufficient security measures,[244] as evaluated through the "information security obligation" (discussed below).[245] Such requirements are an ongoing duty — where a TPP fails to maintain them after accreditation; the ACCC can revoke, suspend or impose conditions upon their status as an ADR.[246]

While the legislation itself features some of these protection principles,[247] the CDR framework also contains the flexibility to react to emerging privacy and security risks.[248] This is achieved by way of rule-making (e.g., the CDR

240. Also note the penalties available for enforcement under the PSR: the FCA may impose a financial penalty corresponding to those under the Financial Services and Markets Act 2000 (PSR arts. 111, 112, ¶ 6), cancel a PSP's authorization (art. 10), publish a statement of public censure (art. 110) or seek an injunction (art. 113). PSR, *supra* note 141, arts. 10, 111, 112, ¶ 6, 113.

241. OFF. OF THE AUSTL. INFO. COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, CHAPTER 12: PRIVACY SAFEGUARD 12 – SECURITY OF CDR DATA, AND DESTRUCTION OR DE-IDENTIFICATION OF REDUNDANT DATA 3 (2020) (stating that securing this data is important to ensure that it is not misused, lost, accessed without authorization, or modified).

242. *Competition and Consumer Act*, *supra* note 91, s 56BD(1)(b). While transfers of data out of the CDR system are possible, it is highly restricted. THE TREASURY (AUSTL.), CONSUMER DATA RIGHT PRIVACY PROTECTIONS 5 (2018) [hereinafter THE TREASURY (AUSTL.), CDR PRIVACY PROTECTIONS], https://treasury.gov.au/sites/default/files/2019-03/CDR-Privacy-Summary.pdf.

243. Accreditation criteria are set by the ACCC pursuant to section 56BH(1) of the Competition and Consumer Act. *See also Consumer Data Rules*, *supra* note 88, pt 5.

244. THE TREASURY (AUSTL.), CDR PRIVACY PROTECTIONS, *supra* note 242, at 5; Explanatory Memorandum, CDR Bill, *supra* note 71, at 20.

245. ACCC, CDR SUPPLEMENTARY GUIDELINES: INFORMATION SECURITY, *supra* note 92, at 5.

246. THE TREASURY (AUSTL.), CDR PRIVACY PROTECTIONS, *supra* note 242, at 5 (explaining the ACCC's oversight power); OFF. OF THE AUSTL. INFO. COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241 (stating that, if the applicant does not remain compliant with Privacy Safeguard 12, its accreditation may be revoked).

247. While Safeguards 1 to 11 largely aim to address privacy concerns, Safeguard 12 also addresses security concerns. *Competition and Consumer Act*, *supra* note 91, s 56 EO(1).

248. THE TREASURY (AUSTL.), CDR PRIVACY PROTECTIONS, *supra* note 242, at 4

Rules) and standard-setting processes (e.g., the "Data Standards").[249] The Rules are made by the ACCC to flesh out the substantial requirements of the scheme,[250] while the Data Standards help to ensure functionality and security at a practical level.[251] In contrast to the UK's private, industry-funded OBIE, these are developed by a government-appointed Data Standards Chair[252] with assistance from a public Data Standards Body[253] (currently the CSIRO's "Data 61" team).[254] Nonetheless, there is still room for industry input in developing the Standards, with the Chair using his powers to establish a Banking Advisory Committee.[255]

The CDR regime's "information security obligation" imposes requirements that resemble those of its EU/UK counterpart. It requires an ADR to take appropriate measures to protect CDR data "from misuse, interference and loss, and from unauthori[z]ed access, modification and disclosure," with minimum steps outlined in the CDR Rules.[256] Like in the EU/UK regime,[257] these minimum requirements mean that an ADR must — at least annually — identify potential security risks and detail the mitigation measures they have implemented in response.[258] Similar to various other PSD II requirements,[259] an accredited person must also establish processes

(explaining the flexibilities in the framework to respond to risks).

249. *Id.* The Consumer Data Rules are made by the ACCC. *See Competition and Consumer Act*, *supra* note 91, s 56BA. The Data Standards are made by the Data Standards Chair. *See id.* s 56FA.

250. For example, the Rules prescribe requirements for collection, disclosure, and use of CDR data. *See id.* s 57BB.

251. For example, the Standards may prescribe the processes and format for data transfer (among other things). *See id.* s 56FA(1); Explanatory Memorandum, CDR Bill, *supra* note 71, at 7, 48.

252. *Competition and Consumer Act*, *supra* note 91, s 56FA(1).

253. *Id.* s 56FK(1).

254. *See Consumer Data Standards*, CSIRO, DATA61, https://data61.csiro.au/en/Our-Research/Focus-Areas/Special-Projects/Consumer-Data-Standards (last updated Jul. 3, 2020).

255. This Committee includes banks, consumer, and Fintech representatives. *See Competition and Consumer Act*, *supra* note 91, s 56FH(2)(a); THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT: CONSUMER DATA RIGHT 52 (2019) [hereinafter THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT]; *Banking Advisory Committee*, CONSUMER DATA STANDARDS, https://consumerdatastandards.org.au/about/advisory-committee/ (last visited July 16, 2021).

256. *Consumer Data Rules*, *supra* note 88, r 5.12, sch 2 item 1.3; ACCC, CDR SUPPLEMENTARY GUIDELINES: INFORMATION SECURITY, *supra* note 92; see also *Consumer Data Rules*, *supra* note 88, sch 2 for the minimum requirements.

257. PSD II, *supra* note 1, art. 95(2) at 104. Under PSD II, the PSP must also provide this assessment to their competent authority.

258. *Consumer Data Rules*, *supra* note 88, sch 2 item 1.3.

259. The EU/UK regime requires "strong customer authentication," "strong and

to limit unauthorized access (including multi-factor authentication for all access to CDR data other than by the data's CDR consumer), secure their network and systems (including by use of encryption), and implement a formal program to identify and remediate vulnerabilities quickly.[260] Such security capabilities must be reviewed and adjusted at least annually, or more frequently where there has been a "material change" in the nature and extent of threats.[261] Lastly, and again analogously to its EU/UK counterpart,[262] the Rules require incident management and reporting in the form of "CDR data security response plans."[263] Such procedures must detect and respond to information security incidents "as soon as practicable."[264] They must also involve the notification of "eligible data breaches"[265] to the Information Commissioner and to affected consumers where required[266] and "information security incidents" to the Australian Cyber Security Centre.[267]

The most salient feature in the CDR regime is perhaps the thirteen Privacy Safeguards ("PSs") introduced by the CDR Act.[268] While the PSD II/PSR regime contains several provisions on data protection, the CDR Act goes one step further by creating its own privacy protection mechanism. These legally binding statutory provisions are inserted into the Competition and Consumer Act 2010 itself,[269] setting out rights and obligations in relation to collecting,

---

widely recogni[z]ed" encryption techniques, and internal control mechanisms to detect and classify security incidents. *See* PSD II, *supra* note 1, arts. 95(1), 97 at 104, 106; RTS, *supra* note 98, art. 35(1) at 41.

260. *Consumer Data Rules*, *supra* note 88, sch 2 item 2.2.

261. *Id*. item 1.5(2).

262. The EU/UK regime requires PSPs to maintain effective incident management procedures and report major incidents to the competent authority. *See* PSD II, *supra* note 1, arts. 95(1), 96(1) at 104–05.

263. *Consumer Data Rules*, *supra* note 88, sch 2 item 1.7(2).

264. *Id.* item 1.7(1).

265. An "eligible data breach" is a data breach "likely to result in serious harm to any of the individuals to whom the information relates." *Privacy Act 1988*, *supra* note 112, s 26WE.

266. *Consumer Data Rules*, *supra* note 88, sch 2 item 1.7(3)(b); *see also Privacy Act 1988*, *supra* note 112, pt IIIC.

267. "In any case, this notification must occur no later than 30 days after the ADR becomes aware of the security incident." *Consumer Data Rules*, *supra* note 88, sch 2 item 1.7(3)(c).

268. OFF. OF THE AUSTL. INFO, COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER A: INTRODUCTORY MATTERS 4 (listing the thirteen Privacy Safeguards).

269. *See Competition and Consumer Act*, *supra* note 91, div 5; OFF. OF THE AUSTL. INFO, COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER A: INTRODUCTORY MATTERS 4.

holding, using, and disclosing CDR data.[270] They are more onerous than the long-established APPs under the Privacy Act 1988.[271] Several broader points can be drawn here. First, the interplay between the PSs and the APPs/Privacy Act can be even more complicated than its EU/UK counterpart. In some instances, the PSs operate alongside the APPs, while in others, the PSs operate to exclude the APPs.[272] Specifically, the application of PSs depends on the context — for instance, while they primarily apply to ADRs, they are also applicable to data holders concerning their handling of the CDR data.[273] Moreover, the obligations imposed could vary depending on the CDR entity. For instance, while APP 1 sets forth overall privacy management for all APP entities,[274] PSs have different requirements for a CDR data holder (i.e., banks) and an ADR (i.e., TPPs).[275] This is to ensure that "there are no gaps" in data protection under the CDR regime.[276]

Second, the CDR regime features various GDPR-style protections. The PSs, for instance, cast a wider net by applying to CDR data that *relates to* individuals or entities,[277] while the APPs apply to "personal information" that is *about* an identified or "reasonably identifiable" individual.[278] The

270. OFF. OF THE AUSTL. INFO, COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER A: INTRODUCTORY MATTERS at 4. Note that the Safeguards "only apply to data for which there are one or more consumers" (consumer data) rather than product data. *Competition and Consumer Act*, *supra* note 91, s 56EB(1).

271. *Compare Privacy Act 1988*, *supra* note 112 (setting out what constitutes an APP breach but not identifying the safeguards in place), *with Competition and Consumer Act*, *supra* note 91, div 5 (stating both of the privacy safeguards that are in position to protect CDR consumers and their data).

272. Explanatory Memorandum, CDR Bill, *supra* note 71, at 54–66 (stating that the privacy safeguards are in place to operate with the APPs; however, noncompliance may result in the privacy safeguards excluding the APPs).

273. Almost all PSs (barring 3 and 4) apply to ADRs, while only PSs 1, 10, 11, and 13 apply to data holders (when handling CDR data). OFF. OF THE AUSTL. INFO, COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER A: INTRODUCTORY MATTERS 6.

274. An "APP entity" is defined in section 6 of the Privacy Act as "a [Commonwealth] agency or organi[z]ation." In this context, "organi[z]ation" excludes businesses that had a turnover of less than $3,000,000 AUD in the last financial year ("small businesses"). *Privacy Act 1988*, *supra* note 112, ss 6C, 6D.

275. *Competition and Consumer Act*, *supra* note 91, s 56ED(4)–(5).

276. OFF. OF THE AUSTL. INFO, COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER A: INTRODUCTORY MATTERS 7. *Competition and Consumer Act*, *supra* note 91, s 56EC indicates several scenarios where the APP do not apply in the CDR context.

277. *Competition and Consumer Act*, *supra* note 91, ss 56AI(3), 56EB(1); Explanatory Memorandum, CDR Bill, *supra* note 71, at 7.

278. *Privacy Act 1988*, *supra* note 112, s 6, sch 1. It is arguable whether social media platforms' collection of location data, or fitness trackers' collection of heart rate and

GDPR applies to "data controllers" and "data processors,"[279] while PSs likewise apply to data holders and recipients — which, like its EU/UK counterpart, includes "small business[es]."[280] More crucially, the PSs enhance privacy protection in various aspects.[281] For instance, both the GDPR and PSs require "express consent,"[282] while implied consent is also allowed under the APPs.[283] However, the CDR is more restrictive than the GDPR — it does not permit the non-consent-based collection, use, or transfer on grounds like "legitimate interests" of the businesses.[284] Furthermore, like the GDPR,[285] the CDR regime gives any persons affected (including individuals) the standing to sue for CDR breaches — including privacy breaches.[286] Also, similar to the GDPR,[287] contravention of most PSs may attract severe civil penalties.[288] Relating to this is that the CDR

sleep pattern data, would fall within the scope of personal information. MEESE ET AL., *supra* note 115, at 7. This contrasts to the GDPR and CDR — specifically, "personal data" as defined under article 4(1) of the GDPR, or CDR data as defined under section 56AI *Competition and Consumer Act* — which both clearly cover indirect data. *See id.* at 7, 9.

279. GDPR, *supra* note 108, arts. 2–3 at 32–33.

280. Unlike the APPs which do not apply to "small businesses," the PSs bind CDR entities regardless of size. *See Competition and Consumer Act*, *supra* note 91, ss 56ED–56EO; THE TREASURY (AUSTL.), CDR PRIVACY PROTECTIONS, *supra* note 242, at 4.

281. *See* THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT, *supra* note 255, at 12.

282. *Consumer Data Rules 2020* (Cth) rr 4.9, 4.11 (Austl.); GDPR, *supra* note 108, arts. 4(11), 6(1)(a), 7 at 34, 36–37.

283. *Privacy Act 1988*, *supra* note 112, ss 16A, 16B.

284. Under GDPR article 6(1)(f), processing may be lawful if it is necessary for "legitimate interests pursued by the controller."

285. GDPR, *supra* note 108, art. 82 ("Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for damages suffered.").

286. *Competition and Consumer Act*, *supra* note 91, s 56EY ("A person who suffers loss or damage . . . by an act or omission . . . may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention."). There is no such right under the Privacy Act. THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT, *supra* note 255, at 98–99.

287. GDPR article 83(5) breaches can lead to fines of up to €20,000,000 or, "in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

288. *Competition and Consumer Act*, *supra* note 91, s 56EV. Breaches can lead to fines up to $500,000 AUD for individuals or $10,000,000 AUD for corporations, or three times the total value of the benefits that have been obtained, or 10% of the annual domestic turnover of the entity committing the breach (whichever is greater). This is vastly increased compared to the Privacy Act's civil penalty of "2000 penalty units" in section 13G, which is only for serious or repeated breaches.

regime has a wider geographical jurisdiction than the Privacy Act/APPs.[289]

New concerns, however come hand in hand with these improvements. The most obvious one is the complexity of the multi-tier privacy framework with personal information regulated by the APPs, a broader set of data governed by the PSs, and common law playing a role as well.[290] The overall result can be "a series of overlapping and confusing processes and policies," which can complicate compliance for consumers and businesses and hence increase transaction costs.[291] One solution is to overhaul the Privacy Act and APPs entirely rather than introducing a parallel framework.[292] Another sticky point is the "silent party's data" problem. Like its EU/UK counterpart, the Australian Treasury has highlighted this concern by stating that "[r]ules may provide requirements for consent by silent parties, balancing the competing data rights of the parties, and may provide rules restricting certain uses of data (e.g., profiling of silent parties)."[293] The OAIC Privacy Guidelines make clear that it is prohibited to use CDR data "for the purpose: of identifying; compiling insights in relation to; or building a profile in relation to; any identifiable person who is not a CDR consumer who made the consumer data request" (including via aggregating the CDR data), unless the ADR obtains required consent.[294]

289. The CDR regime applies to "some cases where there would not be an Australian link for the purposes of the Privacy Act" — for instance, "where data is collected by a foreign company, outside of Australia, on behalf of an Australian registered company or an Australian citizen, the CDR would apply, but the Privacy Act would not." THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT, *supra* note 255, at 158.

290. MEESE ET AL., *supra* note 115, at 28 (noting that this "complicated legal framework" will be difficult for businesses to comply with and confusing for Australians).

291. *Id.* (advocating that the Australian Government implement a different approach to alleviate some of these challenges).

292. *See, e.g.*, *id.* at 28 (recommending options for the Australian Government to assist businesses while acting efficiently); BUS. COUNCIL OF AUSTL., SUBMISSION NO. 9, RESPONSE TO THE TREASURY LAWS AMENDMENT (CONSUMER DATA RIGHT) BILL 2018 (SECOND STAGE) 8 (Feb. 28, 2019).

293. THE TREASURY (AUSTL.), PRIVACY IMPACT ASSESSMENT, *supra* note 255, at 123.

294. OFF. OF THE AUSTL. INFO. COMM'R, CDR PRIVACY SAFEGUARD GUIDELINES, *supra* note 241, at CHAPTER 6: PRIVACY SAFEGUARD 6 — USE OR DISCLOSURE OF CDR DATA BY ACCREDITED DATA RECIPIENTS OR DESIGNATED GATEWAYS 11; *Consumer Data Rules*, *supra* note 88, r 4.12(3)–(4).

E. Is Screen Scraping Still Legal?

Another controversial issue is the legality of screen scraping after both jurisdictions formalize data sharing through the Open Banking initiatives,[295] as detailed below.

i. EU/UK Model

In the EU/UK, while the PSD II seeks to make screen scraping redundant as more firms begin to use open APIs, the Directive itself does not prohibit it.[296] Instead, such accessibility is regulated in the RTS, which spells out the specific requirements for communication channels in Section 2.[297] As a general rule, from the date that the RTS came into effect on September 14, 2019, TPPs' access to accounts must take one of the authorized forms.[298] Banks are required under the RTS to ensure access and prepare an interface for these third-party providers — either by creating a dedicated API or modifying their existing interface (enabling TPPs to identify themselves).[299] The latter can be seen as screen scraping in a "new, modified form" and has sometimes been referred to as "screen scraping plus."[300] Banks must now ensure that their interfaces comply with these communication standards.[301] Despite the dedicated APIs, there are still concerns that such an interface could be unavailable or not performing to the required standard.[302] This gives rise to the "fall-back" option — banks must permit this type of third-party access until the dedicated interface is restored to the required level of availability and performance.[303]

Controversy about the presence of this fall-back option — with the EBA

---

295. *See generally* Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment*, 30 WASH. INT'L L. J. 28 (2020) (comparing regulatory frameworks among different countries and arguing that data sharing initiatives could reduce demand for screen scraping).

296. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 125–26.

297. *See* RTS, *supra* note 98, § 2 at 37–42 ("Specific requirements for the common and secure open standards of communication.").

298. *Id.* art. 38(2) at 42; Zunzunegui, *supra* note 59, at 29.

299. RTS, *supra* note 98, art. 31 at 38. Note that a TPP has an obligation to identify itself under PSD II articles 66(3)(d) and 67(2)(c).

300. Adam Polanowski & Przemyslaw Gruchala, *Can a User's Account be Accessed Through Screen Scraping?*, NEWTECH LAW (Mar. 15, 2019), https://newtech.law/en/can-a-users-account-be-accessed-through-screen-scraping/.

301. Zunzunegui, *supra* note 59, at 29.

302. RTS, *supra* note 98, art. 33 at 39–40.

303. *Id.* art. 33(4) at 39.

opposing it and the European Commission in favor of it[304] — led to it being tempered with an exemption under Article 33(6) of the RTS.[305] Under this provision, banks can be exempted from the requirement that they implement the fall-back mechanism if they can demonstrate that they meet four conditions: they have complied with Article 32's requirements for dedicated interfaces, have stress-tested the dedicated interface for at least six months, proven wide usage by TPPs for at least three months, and have resolved any problems with the dedicated interface without undue delay.[306] If all of these requirements are met, the competent national authority (in the UK, the FCA) may provide an exemption, such that the bank is not required to allow screen scraping as a fall-back option.[307] In accessing the data held by such banks, PSPs are thus not permitted to use screen scraping under any circumstances.[308]

In short, TPPs may legitimately employ screen scraping plus (which identifies the TPP and thus complies with PSD II requirements) where a bank modifies their existing interface for this purpose rather than creating an API.[309] Where the bank instead creates an API for data access, screen scraping can only be conducted in narrow circumstances — specifically, where the API is not performing to the required standard.[310] The legality of screen scraping is even further restricted where a bank has implemented a compliant, stress-tested, and widely-used API. In such cases, the FCA can provide an exemption to the fall-back provision, ensuring that accessing bank-held data via screen scraping will always be prohibited.[311]

ii. Australian Model

The role of screen scraping is less evident in Australia, with CDR legislation being silent on the issue. Rather than prohibiting or endorsing

304. Screen scraping was prohibited entirely in the EBA's original draft. Rationales included that TPPs using screen scraping were in violation of the obligation to identify themselves under PSD II articles 65(3)(d), 67(2)(c), and that they gained access to information unnecessary for the provision of service. However, certain stakeholders lobbied against this total ban, leading the European Commission to introduce the fallback provision in a later draft of the RTS. *See* Wolters & Jacobs, *supra* note 188, at 36.

305. *Id.*; EUR. BANKING AUTH., GUIDELINES ON THE CONDITIONS TO BENEFIT FROM AN EXEMPTION FROM THE CONTINGENCY MECHANISM UNDER ARTICLE 33(6) OF REGULATION (EU) 2018/389 (RTS ON SCA & CSC) 3 (2018).

306. RTS, *supra* note 98, art. 33(6) at 40.

307. *Id.*

308. Wolters & Jacobs, *supra* note 188, at 36.

309. *See* RTS, *supra* note 98, arts. 30–31 at 37–38. The obligation for a TPP to identify itself is imposed under PSD II articles 66(3)(d) and 67(2)(c).

310. *See* RTS, *supra* note 98, art. 33 at 39–40.

311. *Id.* art. 33(6) at 40; Wolters & Jacobs, *supra* note 188, at 36.

this practice, the Farrell Review recommended Open Banking should aim to make the practice redundant by facilitating more efficient data transfer mechanisms.[312] More recently, the Australian Securities and Investments Commission ("ASIC") expressed that it has no intention to prevent screen scraping, though it has foreshadowed in its recently released Consultation Paper 341 that customers will be liable for loss arising from authorized transactions following the use of screen scraping under certain circumstances.[313] However, despite its apparent legality in this sense, there is some uncertainty about the resulting liability where screen scraping has been used. For instance, as mentioned above, the ASIC has noticed that by providing their login details, a consumer could be in breach of the standard banking terms and conditions for non-disclosure of passwords, thus potentially losing their protection under the ePayments Code and becoming liable for losses that occur.[314] This issue was also identified in the Farrell

312. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at x (noting that "customer data should be transferred via APIs" in accordance with appropriate rules and standards).

313. Joseph Brookes, *Fintechs Get 'Screen Scraping' Green Light From Australian Regulators*, WHICH-50 (Mar. 3, 2020), https://which-50.com/fintechs-get-screen-scraping-green-light-from-australian-regulators/ (quoting the Executive Director of the Australian Securities and Investments Commission, Tim Gough: "[the agency] would monitor the market closely but had no plans to prevent screen scraping"); AUSTL. SEC. & INV. COMM'N, CONSULTATION PAPER 341: REVIEW OF THE EPAYMENTS CODE: FURTHER CONSULTATION 36 (2021) [hereinafter ASIC CONSULTATION PAPER 341], https://asic.gov.au/media/eh2fceff/cp341-published-21-may-2021.pdf ("It is not a prohibition on the use of screen scraping but clarifies the position that a consumer takes particular actions at their own risks.").

314. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 51. ePayments Code section 11.2 states that where a bank can "prove on the balance of probabilities that a user contributed to the loss through . . . breaching the pass code security requirements in clause 12," the customer is liable in full. Clause 12 requires that a customer does not "voluntarily disclose pass codes to anyone," which is breached when providing a TPP with security credentials so that they may use screen scraping technology. More recently, Australian Senate's Select Committee on Financial Technology and Regulatory Technology, in its interim report, suggested that "an outright ban on screen scraping is not prudent at the present time, . . . in many cases these practices are enabling companies to innovate and provide competition in the financial services sector. This situation should continue to be monitored, however, as Open Banking is rolled out." SENATE SELECT COMM. ON FIN. TECH. & REGUL. TECH., INTERIM REPORT (2020) [hereinafter SENATE SELECT COMM., INTERIM REPORT], https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024366/toc_pdf/SelectCommitteeonFinancialTechnologyandRegulatoryTechnology.pdf;fileType=application%2Fpdf. As noted above, while ASIC has no plan to ban screen scraping, it has indicated that customers will have to bear the risks in using screen scraping if (i) the use of that service "amounted to 'disclosure' of the consumer's passcode; and (ii) the subscriber (i.e., banks that subscribe to the e-Payment Code) can "prove on the balance of probability that the use of that services contributed to the loss." ASIC CONSULTATION PAPER 341, *supra* note 313, at 36.

Review.[315]

It seems a shame that the Australian government did not phase out screen scraping or at least keep it as an exception. For one, allowing screen scraping could essentially create two-tiered system where scrapers would continue to utilize this technique, which runs counter to other government security advice,[316] undermines the purpose of the consumer data right,[317] and could result in the loss of protections under the ePayments Code.[318] For another, it would provide little, if any, incentive for some fintech players to seek accreditation if they could instead rely on screen scraping, resulting in financially vulnerable people continuing to engage with non-CDR accredited entities bound by lower privacy protections.[319] However, one should also bear in mind the potential anti-competitive effects associated with a total ban — which seems more feasible until the CDR regime becomes mature.[320] This is especially so considering that the Australian economy heavily relies on screen scraping as a cost-effective tool.[321]

---

315. THE TREASURY (AUSTL.), REVIEW INTO OPEN BANKING, *supra* note 15, at 52 (stating that customers may not be "aware precisely what they've done in providing their login details in this way").

316. FIN. RIGHTS LEGAL CTR. & CONSUMER ACTION L. CTR., SUBMISSION NO. 36, COMMENT ON THE SENATE SELECT COMMITTEE ON FINANCIAL TECHNOLOGY AND REGULATORY TECHNOLOGY'S INQUIRY INTO FINANCIAL TECHNOLOGY AND REGULATORY TECHNOLOGY 12 (2019) (arguing that the practice is "exactly opposite to every other piece of online safety and security advice").

317. *Id.* at 16 (noting that the Consumer Data Right creates "a fundamental right to port and transfer one's own personal financial data . . . but in a safe environment" and "[w]ithout a ban on screen-scraping . . . there is very little incentive for businesses . . . to use CDR accredited software over screen scaping technology").

318. *Id.* at 14 (indicating that "providing access to one's banking data using screen scraping technology amounts to a breach of the terms and conditions of a customer's bank account, and places customers at risk of losing their protections under the E-Payments Code" under section 11.2).

319. *Id.* at 16–17 (providing a quote from FinTech Australia, which notes that "many fintech companies are happy with existing screen scraping solutions, and are likely to continue to use these solutions").

320. FINTECH AUSTL., SUBMISSION NO. 19, SUBMISSION PAPER: SENATE ISSUES PAPER RESPONSE 35 (2019) (arguing that banning screen scraping would be anticompetitive as screen scraping is the most "secure, economical, accessible, and accepted system by which fintechs can and do seek information").

321. FINTECH AUSTL., SUBMISSION PAPER: SUBMISSION TO OPEN BANKING INQUIRY 9 (2017) (noting that the most successful companies are those that can access and utilize consumer data, increasingly so in the financial services industry, and outlawing screen scaping will harm Australian companies' ability to do so and compete with other companies internationally). According to FinTech Australia, to be CDR accredited receipts, it would cost between $100,000 AUD to $250,000 AUD. Thus, it suggested that "CDS must be implemented in a way that is 'easier to access, provides better functionality and is cheaper than screen scraping." On the cost-benefit analysis, see, e.g., FINTECH AUSTL., SUBMISSION PAPER: SUBMISSION TO THE AUSTRALIAN COMPETITION

Overall, while it seems that screen scraping is currently legal as a technique running parallel to the CDR scheme, this is controversial and may be subject to change, with various stakeholders arguing for or against a ban. There is also uncertainty as to liability associated with the practice.[322]

IV. CONCLUSION

While many countries have reacted to the changing landscape by rolling out Open Banking initiatives to tap into the potential of consumer banking data, their responses have taken different shapes. As discussed, although both the UK and Australia have adopted mandatory approaches that require data sharing with certain common features, there are striking differences. While Australia casts a wide net with a cross-sector CDR regime, the UK model applies to only the banking sector — though the recent "Smart Data" initiative reveals that the UK seems to be moving towards the Australian approach by applying data sharing to other sectors. Both regimes apply to a wide range of data to be shared, though Australia has reacted to the industry by excluding materially enhanced information from the scope of data sharing.

The UK maintains a clear framework for allocating liabilities between different parties; it is regrettable, however, that Australia's CDR has no such comparable system yet. Both jurisdictions have dedicated frameworks dealing with security and data protection issues; yet, the relationship between the PSs and Privacy Act/APPs in Australia is rather complicated for compliance. Screen scraping is generally banned in the UK except for the fall-back option. However, it is not yet prohibited in Australia, given that many online businesses still heavily rely on this handy tool for their operations. While it may be too early to judge which model will prevail, it is clear that the Australian model missed the opportunity to tackle some of the more critical issues head-on. These nuanced differences may nevertheless help other jurisdictions reflect on their regulatory approaches in this data-driven shifting landscape.

AND CONSUMER COMMISSION CONSUMER DATA RIGHT- PARTICIPATION OF THIRD[-]PARTY SERVICE PROVIDERS (2020), https://www.accc.gov.au/system/files/CDR%20Rules%20-%20Intermediaries%20consultation%20submission%20-%20Fintech%20Australia%20REDACT.pdf; SENATE SELECT COMM., INTERIM REPORT, *supra* note 314, at 152.

322. However, ASIC's acting Executive Director recently told the Senate Committee that there is "no evidence of which we're aware of any consumer loss from screen scraping." *See* Brookes, *supra* note 313.