Journal of Business & Technology Law

Volume 17 | Issue 2 Article 3

Embedding Open Banking in Banking Law: Responsibilities, Performance, Risk and Trust

Scott Farrell

Embedding Open Banking in Banking Law: Responsibilities, Performance, Risk and Trust

SCOTT FARRELL*©

ABSTRACT

Open banking is an evolving trend in many jurisdictions and is about to commence in the United States too, with the issuance by the Consumer Financial Protection Bureau of an advance notice of proposed rulemaking, and the Executive Order on Promoting Competition in the American Economy. Whilst there are many practical and technological issues to address in establishing these frameworks to enable customers to share their banking data as they choose, fundamental legal issues also need to be addressed. These arise out of the data portability, customer autonomy and recipient accountability functions at the foundation of open banking. The legal design that supports open banking is critical to enabling the performance of these functions, and the achievement of the competition, innovation and consumer protection objectives of open banking frameworks.

This article focuses on the legal design of the recipient accountability function of open banking by analysing the legal responsibilities for the data which has been shared. It does this by comparing key aspects of those legal responsibilities in two common law countries where open banking is already in operation, Australia and the United Kingdom ('UK') and evaluating those responsibilities against those applicable to the custody of transferred funds under banking law. This evaluation is intended to demonstrate how a jurisdiction's own banking law can be used as an important reference point in designing open banking's legal architecture in a jurisdiction in which it is new, such as the United States. It also reveals that the exposure which customers take on the performance of these responsibilities by their data recipients is greater than that which they take on their bank with respect to their funds under banking law and explores how the ways those risks are managed in banking can be adapted for open banking to support customer trust.

* Adjunct Professor, School of Private and Commercial Law, UNSW Sydney.

I would like to thank Scientia Professor Ross Buckley; Professor Douglas Arner; and Dr Anton Didenko for their ideas and guidance, and Jack Zhou and Vien Siu for their able research assistance. All responsibility is mine.

Embedding Open Banking in Banking Law

TABLE OF CONTENTS

Embedding Open Banking in Banking Law

I. INTRODUCTION

Open banking is an 'evolving trend in many jurisdictions,' [1] and is about to commence in the United States too, with the issuance by the Consumer Financial Protection Bureau ('CFPB') of an advance notice of proposed rulemaking ('ANPR'),[2] and the Executive Order on Promoting Competition in the American Economy.[3] Whilst there are many practical and technological issues to address in establishing a framework to enable customers to share their banking data as they choose,[4] fundamental legal issues also need to be addressed. These are out of the core data portability, customer autonomy and recipient accountability functions performed by open banking. The legal design which supports open banking is critical to enabling the performance of these functions, and the achievement of the competition, innovation, and consumer protection objectives of open banking.

This article examines the legal design requirements of the recipient accountability function of open banking by analysing the legal responsibilities for the data which has been shared under open banking. It does this by comparing key aspects of the legal responsibilities in two common law countries where open banking is already in operation, Australia and the United Kingdom ('UK'); evaluating those responsibilities against those applicable to the custody of transferred funds under banking law. This evaluation reveals that the exposure customers take on the performance of open banking responsibilities relating to their data is greater than their exposure to the performance of monetary responsibilities relating to their funds. It also explores how the way that these risks are managed in banking can be adopted for use in open banking to support customer trust. This analysis and evaluation are intended to demonstrate how a jurisdiction's own banking law can be used as an important reference point in designing open banking's legal architecture in a jurisdiction in which it is new, such as the United States.

1. Bank for Int'l Settlements, *Report on Open Banking and Application Programming Interfaces*, at 4 (Nov. 2019), https://www.bis.org/bcbs/publ/d486.pdf [hereinafter *BIS Report*]; These jurisdictions include Australia, Brazil, Canada, the European Union, Hong Kong, India, Israel, Japan, Malaysia, Mexico, New Zealand, Nigeria, Russia, Singapore, South Korea and the United Kingdom. *Id.* at 8 n.5; *Open Banking Countries,* OPEN BANKING TACKER, https://www.openbankingtracker.com/countries (last visited Apr. 8, 2022).

2. Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020) (seeking "comments . . . to assist the Bureau [of Consumer Financial Protection] in developing regulations to implement [S]ection 1033" of the Dodd- Frank Wall Street Reform and Consumer Protection (Dodd-Frank) Act, 12 U.S.C. § 5533).

3. Exec. Order No. 14,036, 86 Fed. Reg. 36,987, 36,998 (July 9, 2021).

4. Such as how access is to be provided, what data is covered, in what form it is provided, how the holding and use of the information is controlled, the security and accuracy of the shared data, and the transparency of the data sharing. Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020); *See also* CHERYL R. COOPER, CONG. RSCH. SERV., IN11745, OPEN BANKING, DATA SHARING, AND THE CFPB'S 1033 RULEMAKING 2-3 (2021).

Part 1 of this article lays the foundation of the analysis by introducing open banking, its three key functions, its alignment with banking law and introduces the basis of the legal responsibilities for shared data under open banking frameworks of Australia and the UK. The following parts use this foundation to compare key aspects of the legal responsibilities under Australian and UK open banking and evaluate them against banking law. These relate to the legal responsibilities in requesting customer data (Part 3), in using shared customer data (Part 4), for the integrity of shared customer data (Part 5), and in authorization to receive customer data (Part 6). Conclusions are drawn in Part 7 on the implications for performance, risk and trust for open banking arising from the analysis.

II. Foundation of Analysis – Introduction to Open Banking

1. Meaning and Functions of Open Banking

Open banking has no widely accepted legal definition.[5] It is not defined in the legislative instruments which establish and govern open banking in the UK and Australia,[6] the legislative instrument of its foundation in the EU,[7] or the documents which form its foundation in Hong Kong,[8] or Singapore.[9] Even the Dodd-Frank Act does not attempt a definition.[10] Instead, it is more common for open banking's purpose to be described than for its meaning to be defined. For example, the Congressional Research Service describes open banking as 'the practice of giving financial services firms access to customer banking and other financial data to facilitate the development of new types of products and services for consumers.'[11] The Bank for International Settlements ('BIS') describes open banking as:

5. *See, e.g.*, Nydia Remolina, *Open Banking: Regulatory challenges for a New Form of Financial Intermediation in a Data-Driven World* 9-10 (SMU Ctr. for AI and Data Governance, Research Paper No. 5, 2019) (Sing.); Christopher C. Nicholls, *Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation*, 35 BANKING & FIN. L. R. 121, (2019); Alessandro Palmieri & Blerina Nazeraj, *Open Banking and Competition: An Intricate Relationship*, 5 E.U. & COMPAR. L. ISSUES & CHALLENGES SERIES 217, 218 (2021); Ross P. Buckley et al., *Australia's Data-Sharing Regime: Six Lessons for the World*, 33(1) KING'S L. J. 61-91, 64 (2022); DANIEL GOZMAN ET AL., OPEN BANKING: EMERGENT ROLES, RISKS & OPPORTUNITIES 19 (2018).

6. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) (Austl.); *Competition and Consumer Act 2010* (Cth.) (Austl.).

7. Council Directive 2002/65, 2015 O.J. (L 337) 35 (EU) [hereinafter PSD2].

8. H.K. MONETARY AUTH., OPEN API FRAMEWORK FOR THE HONG KONG BANKING SECTOR (2018).

9. ASS'N OF BANKING IN SING. & MONETARY AUTH. OF SING., ABS-MAS FINANCIAL WORLD: FINANCE-AS-A-SERVICE API PLAYBOOK (2016).

10. "Subject to the rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person[.]' Dodd-Frank Wall Street Reform and Consumer Protection Act § 1033, 12 U.S.C. § 5533.

11. *See* COOPER, *supra* note 4, at 1.

> *the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities.*[12]

CGAP (Consultative Group to Assist the Poor), a partnership of development organisations housed and administered by the World Bank,[13] takes a similar approach, describing open banking as 'a consent-based data-sharing scheme mandated or supported by regulators toward the goal of creating competition and fostering innovation in financial services.'[14] These descriptions, and others suggested by scholars,[15] emphasise three functions of open banking:

- *Data portability* – open banking enables customer banking data to be shared.[16] Data portability in open banking is supported using interoperable standardized data technology,[17] primarily Application Programming Interfaces (or 'APIs');[18]

12. *BIS Report*, *supra* note 1, at 4 n.1.

13. *About CGAP: Our Governance*, CONSULTATIVE GRP TO ASSIST THE POOR (2022), https://www.cgap.org/about/governance.

14. Ariadne Plaitakis & Stefan Staschen, Open Banking: How to Design for Financial Inclusion 4 (October 2020) (working paper) (on file with the Consultative Group to Assist the Poor).

15. *See*, *e.g.*, Ana Badour & Domenic Presta, *Open Banking: Canadian and International Developments*, 34 BANKING & FIN. L. R. 41, 42 (2018); *See also* Fernando Zunzunegui, *Digitalisation of Payment Services* 11-13 (Ibero-Am. Inst. for Law & Fin., Working Paper No. 1/2018, 2018); Nicholls, *supra* note 5.

16. Open banking might also be described as a form of data access, but the distinction is not relevant here. *See* Inge Graef, et al., *Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes* 18 (Tilburg L. & Econ. Ctr., Tilburg Univ., Discussion Paper No. DP 2019-005, April 2019); *But see* Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 COMPUT. L. & SEC. REV. 193, 201-02 (2018).

17. Unlike data portability under *GDPR*, open banking requires that data be shared in a standardised form which is interoperable between technology systems (syntactic portability) and meaningful to the recipient (semantic interoperability). *See* Regulation 2016/679, 2016 O.J. (L119) 1 [hereinafter *GDPR*]; Christian Reimsbach-Kounatze, *Enhancing Access to and Sharing of Data: Striking the Balance Between Openness and Control Over Data*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 27, 27-33 (Ger. Fed. Ministry of Just. & Consumer Prot. & Max Planck Inst. for Innovation & Competition eds., 2021); Heike Schweitzer & Robert Welker, *A Legal Framework For Access To Data: A Competition Policy Perspective*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 103 (Ger. Fed. Ministry of Just. & Consumer Prot. & Max Planck Inst. for Innovation & Competition eds., 2021).

18. *See* Oscar Borgogno & Giuseppe Colangelo, *Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs*, 35(5) COMPUT. L. & SEC. REV. 105314, 1 (2019); APIs enable communication between computer applications, by setting out data available for retrieval and how it can be retrieved. *Id.* at 6. They are "a set of protocols which define how software components communicate with each other." *Id*.; APIs are also known as "the 'Babel Fish' for financial communications." *See* Julian Cork, *Banking as a Platform*, *in* THE BOOK ON OPEN BANKING: A SERIES OF ESSAYS ON THE NEXT EVOLUTION OF MONEY 85, 88 (2018); *See also* Johannes Ehrentraud

- *Customer autonomy* – open banking empowers customers to control the sharing of their customer banking data.[19] Customer autonomy is supported by the legal rights of customers to share their data under open banking; and
- *Recipient accountability* – open banking makes the recipients of shared customer banking data accountable to customers. Recipient accountability is supported by the legal responsibilities of recipients of customer data under open banking.[20]

Whilst the second of these is not the focus of this article,[21] all three are fundamental to the effectiveness of open banking in achieving its competition, innovation and consumer protection objectives.[22] Together they encourage competition and innovation by overcoming the 'data bottleneck problem' created by the 'gatekeeper role' which banks perform by controlling access to customer account information,[23] and by reducing the switching costs for customers and the

et al., *Policy Responses to Fintech: A Cross-Country Overview*, BANK FOR INTERNATIONL SETTLEMENTS: FINANCIAL STABILITY INSTITUTE 33 (Jan. 2020), https://www.bis.org/fsi/publ/insights23.pdf; *BIS Report*, *supra* note 1, at 9.

19. Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 346-49 (2021); Fracassi and Magnusson argue that a data subject 'owning' their data is a necessary part of data autonomy. *Id.* at 9. However, defining the concept of property rights in data is difficult, partly because the essential feature of a right to exclude others is rarely able to be established. *Id.* at 11. *See generally* Nadezhda Purtova, *The Illusion of Personal Data as No One's Property*, 7 L., INNOVATION & TECH., July 2015, at 1, 7; Reimsbach-Kounatze, *supra* note 17; "There are no general data ownership rights in the EU or elsewhere." Bertin Martens, *An Economic Perspective on Data and Platform Market Power* 5 (European Comm'n, Joint Rsch. Ctr. Digit. Econ. Working Paper No. 2020-09, 2021).

20. *See generally* Inge Graef et al., *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, 19 GER. L. J. 1359, 1362 (2018); *BIS Report*, *supra* note 1, at 14-15; However, it differs from the accountability customarily imposed by those laws. This is because the focus of accountability in open banking is to enable value to be provided to the customer through the provision of a particular good or service rather than the protection of fundamental rights of privacy or general rights of control. *See* Laura Somaini, *The Right to Data Portability and User Control: Ambitions and Limitations*, 3 MEDIALAWS 164, 169-70 (2018); Jörg Hoffmann, *Safeguarding Innovatoin Through Data Governance Regulation: The Case of Digital Payment Services*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 343, 349 (Ger. Fed. Ministry of Just. & Consumer Prot. & Max Planck Inst. for Innovation & Competition eds., 2021); Oscar Borgogno & Giuseppe Colangelo, *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking,* 9 J. EUR. CONSUMER & MKT. L. 143, 144 (2020).

21. *See also* Scott Farrell, Designing Open Banking in America: Lessons from Australian and UK Banking Law (Feb. 2, 2022) (unpublished manuscript) (on file with author), for an analysis of the second function.

22. *See* Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020), for expression of these in America; Exec. Order No. 14,036, 86 Fed. Reg. 36,987, 36,998 (July 9, 2021) (discussing the promotion of competition in the American economy).

23. *See* Borgogno & Colangelo, *supra* note 18, at 6; *See also* Julio Martinez, *Open Banking and the Role of Banks*, *in* THE BOOK ON OPEN BANKING: A SERIES OF ESSAYS ON THE NEXT EVOLUTION OF MONEY 74, 77 (2018); AUSTL. COMPETITION & CONSUMER COMM'N., DIGITAL PLATFORMS INQUIRY: FINAL REPORT 115-16 (2019).

'lock-in' to current service providers.[24] Also, they improve consumer protection through enhanced information security (particularly by avoiding the need for 'screen scraping),[25] improving consumers' comprehension of the risks and benefits in sharing their data, [26] and customers' confidence through authorization requirements for data recipients.[27] Importantly for the analysis in this article, these functions of open banking with respect to customer data also align with key functions performed by banks with respect to customer funds.

2. Functional Alignment of Banking and Open Banking

A primary economic function performed by commercial banks is holding customer funds and paying those funds as the customer instructs.[28] This storage and liquidity of customer value is the 'essence of what banks promise to their depositors,'[29] and the foundation of the legal relationship between bank and customer.[30] The legislative, regulatory, contractual, and technological arrangements which enable these functions to be performed have evolved over

24. *See* Giuseppe Colangelo & Oscar Borgogno, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, 31 EUR. BUS. L. R. 573, 577 (2020); *See also* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 338 (2012); Michael McKee et al., *PSD2 and Open Banking - Rewiring the Plumbing of the European Payments Ecosystem*, 35 J. INT'L BANKING L. & REGUL. 85, 89 (2020).

25. Screen scraping involves customers sharing their online banking login credentials when sharing data. *See* Hoffmann, *supra* note 20, at 346; Screen scraping involves customers sharing their online banking login credentials when sharing data. *See* Hoffmann, *supra* note 20; Simonetta Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, *in* COMPETITION AND INNOVATION 39 (V. Bagnoli ed., 2018); Memorandum from the Fin. Servs. Comm. Majority Staff to the Members of the Comm. on Fin. Servs. (Sept. 16, 2021) (on file with author) (providing background information for the Task Force on Financial Technology hearing entitled "Preserving the Right of Consumers to Access Personal Financial Data," which was held on September 21, 2021); However, it remains commonly used. *See* STANDING SENATE COMM. ON BANKING TRADE & COM., OPEN BANKING: WHAT IT MEANS FOR YOU 37 (2019) (Can.).

26. Andrew Dahdal & Bruno Zeller, *Open Banking and Open Data: Global Context, Innovation and Consumer Protection*, July-Aug. 2021, at 1, 17; *See also* PSD2, *supra* note 7, at recital 6.

27. *See infra* Part IV.

28. BENJAMIN GEVA, BANK COLLECTIONS AND PAYMENT TRANSACTIONS: A COMPARATIVE STUDY OF LEGAL ASPECTS 7 (Oxford Univ. Press, 2001).

29. Dan Awrey & Kristin, *The Shadow Payment System*, 43 J. CORP. L. 775, 783 (2018).

30. *See* Foley v. Hill [1848] 9 Eng. Rep. 1002, 1004 (U.K.); Joachimson v. Swiss Bank Corp. [1921] 3 KB 110, 118 (U.K.); Tournier v. Nat'l Provincial and Union Bank of Eng. [1924] 1 KB 461, 484 (U.K); *Laing v. Bank of N.S.W.* (1952) 54 SR (NSW) 41, 43 (Austl.); *Re Austl. and N.Z. Savings Bank Ltd.; Mellas v Evriniadis* [1972] VR 690 (Vict.) (Austl.); *Smorgan v Austl. and N.Z. Banking Group Ltd.; Fed. Comm'n of Tax'n v Smorgon* (1976) 134 CLR 475 (Austl.).

many centuries,[31] so that most money now consists of bank accounts[32] (comprised of bank account data)[33] and most payments are funds transfers[34] (effected by communicating changes to bank account data).[35] In fact, '[b]anks from this perspective, are specialized institutions for facilitating the transmission and recording of relevant payment information.'[36]

This perspective reveals similarities between the functions performed for customer funds in banking and the functions performed for customer data in open banking. With acceptance that data generally, and customer account information more particularly, are valuable,[37] both sets of functions involve information of value to customers, either customer funds or customer data. In each case, the customer can choose to transfer that value (customer autonomy), by the communication of information (data portability), and the recipient is responsible for the custody of the value transferred (recipient accountability). In fact, there is an emerging

31. BENJAMIN GEVA, THE PAYMENT ORDER OF ANTIQUITY AND THE MIDDLE AGES: A LEGAL HISTORY 5 (Hart Publ'g Ltd., 2011); "[M]odern banking in the loan and payment networks can be traced back to the Knights Templar and the Italian renaissance banks." ROSS CRANSTON ET AL., PRINCIPLES OF BANKING LAW 3 (Oxford Univ. Press, 3rd ed. 2017); In addition, safekeeping functions performed by London goldsmiths developed into banking services by the late-seventeenth century. Awrey & van Zwieten, *supra* note 29, at 787.

32. Formerly, bank accounts were not considered to be money from a legal perspective as that characterisation was reserved for legal tender circulating as currency. However, accounts with commercial banks are now commonly considered to be money from a legal perspective. *See* EWAN MCKENDRICK, GOODE ON COMMERCIAL LAW 485-500 (LexisNexis, 4th ed. 2009); CHARLES PROCTOR, MANN ON THE LEGAL ASPECT OF MONEY PC (Oxford Univ. Press, 7th ed. 2012); VICTORIA DIXON, GOODE ON PAYMENT OBLIGATIONS IN COMMERCIAL AND FINANCIAL TRANSACTIONS PC (Sweet & Maxwell Ltd., 4th ed. 2020); DAVID FOX, PROPERTY RIGHTS IN MONEY ¶ 1.38 (Oxford Univ. Press 2008); Anton N. Didenko & Ross P. Buckley, *The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies*, 42 FORDHAM INT'L L.J. 1041, 1058 (2019).

33. *See* Andreas Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin): Suggestions for Definitions*, 34 J. INT'L BANKING L. & REGU., no. 3, 2019 at 1, 2; *See also* Zunzunegui, *supra* note 15, at 14; LUCIANO FLORIDI, THE 4TH REVOLUTION: HOW THE INFOSPHERE IS RESHAPING HUMAN REALITY 46 (Oxford Univ. Press, 2014) (stating that "money may well be just a pile of digits"); *See also* GOTTFRIED LEIBBRANDT & NATASHA DE TERAN, THE PAY OFF: HOW CHANGING THE WAY WE PAY CHANGES EVERYTHING 157 (Elliott & Thompson Ltd., 2021).

34. *See* GEVA, *supra* note 28; *See also* STEPHEN MILLARD ET AL., THE FUTURE OF PAYMENT SYSTEMS (Routledge, 1st ed. 2007).

35. MICHAEL BRINDLE & RAYMOND COX, LAW OF BANK PAYMENTS ¶ 3-002 (Sweet & Maxwell Ltd., 5th ed. 2018); "[N]othing tangible or intangible is transferred." GEVA, *supra* note 31, at 607; Instead, messages, or transfers of *information*, cause the change in the account balances, and rules which govern them are the equivalent of delivery and possession in legal tender. FOX *supra* note 32, at ¶ 3.14.

36. MILLARD ET AL., *supra* note 34, at 68.

37. Vezzoso, *supra* note 25; *See also* Buckley et al., *supra* note 5, at 3; *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security*, INT'L TELECOMM. UNION 1, 12-18 (2018); PRODUCTIVITY COMM'N., INQUIRY REPORT NO. 82: DATA AVAILABILITY & USE 57-64 (2017) (Austl.); ACS, PRIVACY IN DATA SHARING: A GUIDE FOR BUSINESS AND GOVERNMENT 7-13 (2018) (Austl.); Gianclaudio Malgieri & Bart Custers, *Pricing Privacy – The Right to Know the Value of Your Personal Data*, 34 COMPUT. L. & SEC. R. 289, 290 (2018); Org. for Econ. Co-Operation and Dev. [OECD], *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OCED Digital Economy Papers, at 9-10, No. 220 (Apr. 2, 2013); HER MAJESTY'S (HM) TREASURY, DISCUSSION PAPER: THE ECONOMIC VALUE OF DATA, 2018, at 4-7 (UK).

understanding that 'finance, data and technology are now all tethered one to the other,'[38] and 'the financial economy is giving way to the data economy in which handling data is essential to economic success.'[39]

Despite these similarities, there are only limited references in academic works to this functional equivalence between open banking with customer data and banking with customer funds.[40] This article uses this similarity to evaluate the results of its comparative analysis under open banking in Australia and the UK. The legal foundation for open banking in the two jurisdictions is introduced next.

3. Open Banking in Australia and the UK

Open banking was established in the UK in 2017,[41] and in Australia in 2019.[42] The primary objectives for doing so in both jurisdictions were similar to those expressed in America: to improve competition,[43] encourage innovation,[44] and enhance consumer protection.[45] Despite this similarity in purpose, the analysis below shows that the legal foundation of responsibilities for the data shared under open banking in Australia and the UK is significantly different. This difference in legal foundation of open banking between Australia and the UK stands in contrast with the close connection and similarity in their banking laws.[46] Much of banking law in Australia and the UK is based on the common law of contract and agency, which differ little between the two jurisdictions as they have a shared legal heritage. The connection

38. Dirk A Zetzsche et al., *The Evolution and Future of Data-Driven Finance in the EU*, 57 COMMON MKT L.R. 331, 351 (2020).

39. Zunzunegui, *supra* note 15, at 2.

40. *See id.* at 13-14; *See also* INE VAN ZEELAND & JO PIERSON, IN BANKS WE TRUST: BANKS AS CUSTODIANS OF PERSONAL DATA IN OPEN BANKING ECOSYSTEMS 14-15 (2021).

41. Press Release, Competition and Mkts. Auth., Update on Open Banking (Oct. 1, 2021) (on file with author) (U.K.).

42. AUSTL. GOV. COMMONWEALTH TREASURY, INQUIRY INTO FUTURE DIRECTIONS FOR THE CONSUMER DATA RIGHT 1 (2020).

43. *See* Competition and Mkts Auth., *Retail Banking Market Investigation*, GOV.UK (Aug. 9, 2016), https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#responses-to-provisional-decision-on-remedies (providing an example from the U.K.);FIN. CONDUCT AUTH. [FCA], OPEN FINACE 3 (2021) (providing an example from the U.K.); Colangelo & Borgogno, *supra* note 24 (providing an example from the U.K.); Press Release, Scott Morrison, Treasurer, The Treasury, Government Response to the Open Banking Review (May 9, 2018), sjm.miminsters.treasury.gov.au (providing an example from Australia); AUSTL. GOV. COMMONWEALTH TREASURY, REVIEW INTO OPEN BANKING: GIVING CUSTOMERS CHOICE, CONVENIENCE AND CONFIDENCE 9 (2017) (providing an examples from Australia).

44. HER MAJESTY'S (HM) TREASURY, DATA SHARING AND OPEN DATA IN BANKING: RESPONSE TO THE CALL FOR EVIDENCE, 2015, at 5 (providing an examples from the U.K.); AUSTL. GOV. COMMONWEALTH TREASURY, CONSUMER DATA RIGHT OVERVIEW 2 (2019) (Austl.) (providing an example from Australia).

45. *See* McKee et al., *supra* note 24, at 86; *See also* Vezzoso, *supra* note 25, at 34; *See also* AUSTL. GOV. COMMONWEALTH TREASURY, *supra* note 44, at 5-6.

46. *See* PHILIP R. WOOD, COMPARATIVE FINANCIAL LAW 49 (Sweet & Maxwell Ltd. 1995).

is sufficiently close that the analysis of banking law in this article need not distinguish between them.[47] This similarity in banking law, when combined with the similarity in the objectives of open banking and the reliance on data portability, customer autonomy and recipient accountability to achieve them, enables a meaningful analysis of the differences in the legal responsibilities for shared data under open banking between the jurisdictions.

(a) Foundation of Legal Responsibilities Under Australian Open Banking

Open banking in Australia is the first stage of the Consumer Data Right ('CDR'). This is an economy-wide right designed to enable consumers to obtain value from the use of their data.[48] The CDR was established under the *Treasury Laws (Consumer Data Right) Act 2019* (Cth) ('*CDR Act*').[49] The *CDR Act* created a new Part IVD of the *Competition and Consumer Act 2010* (Cth) ('*CCA*'),[50] which can apply to sectors of the Australian economy by designation of the Australian Treasurer through legislative instrument.[51] The *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (Cth) ('*Open Banking Designation*')[52] made such a designation for the banking sector. Following this, the Australian Competition and Consumer Commission ('ACCC') issued the *Competition and Consumer (Consumer Data Right) Rules 2020* ('*CDR Rules*'). The designation, and the *Competition and Consumer (Consumer Data Right) Rules 2020* ('*CDR Rules*') issued by the Australian Competition and Consumer Commission ('ACCC') with respect to it, are the legislative instruments which define the legal right to share banking data under Australian open banking.[53] The *CCA* requires that the 'Data Standards Chair' creates standards ('Australian Standards') for the format and description of shared data and 'the disclosure of shared data.[54]

The responsibilities of a data recipient for the data which have been shared with it under Australian open banking are contained in the *CCA and the CDR Rules.* The *CCA* provides for the *CDR Rules* to include:

47. The principal English cases which form the basis of the banker-customer relationship have been followed and approved by Australian courts. *See* Foley v. Hill [1848] 9 Eng. Rep. 1002, 1002-3 (U.K.); Joachimson v. Swiss Bank Corp. [1921] 3 KB 110, 118 (U.K.); Tournier v. Nat'l Provincial and Union Bank of Eng. [1924] 1 KB 461, 484 (U.K); *Laing v. Bank of N.S.W.* (1952) 54 SR (NSW) 41, 43 (Austl.); *Re Austl. and N.Z. Savings Bank Ltd.; Mellas v Evriniadis* [1972] VR 690 (Vict.) (Austl.); *Smorgan v Austl. and N.Z. Banking Group Ltd.; Fed. Comm'n of Tax'n v Smorgon* (1976) 134 CLR 475 (Austl.).

48. PRODUCTIVITY COMM'N, *supra* note 37, at 15-18.

49. Consumer Data Right) Bill 2019 (Cth) (Austl.).

50. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) (Austl.).

51. *Id*.

52. Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019 (Cth) (Josh Frydenberg, Treasurer) (Austl.) [hereinafter *Open Banking Designation*].

53. The *CDR Rules* is a legislative instrument. *Competition and Consumer Act 2010* (Cth.) s 56BA(1) (Austl.).

54. *Id.* s 56FA(1).

- requirements a person needs to satisfy in order to be disclosed data;[55]
- requirements for the accreditation of data recipients;[56]
- authorization for a person to use data in accordance with the valid consent of a consumer;[57]
- inclusions in the consent for it to be valid, any disclosures, uses or other matters a valid consent may cover, and when a consent ceases to be valid;[58] and
- other rules relating to the disclosure, collection, use, accuracy, storage, security, and deletion of the data.[59]

These provisions apply to CDR Data and CDR Consumers. To be 'CDR data,' the data must be 'within a class of information' designated in the *Open Banking Designation* or is 'wholly or partly' derived from such information.[60] To be a CDR Consumer, it requires that:

- the CDR data relates to the person because of the supply of a good or service to the person or their associates;
- the CDR data is held by, or on behalf of, another person who is a data holder or an accredited data recipient of the CDR data; and
- the person is identifiable, or reasonably identifiable from the CDR data or other information held by that person.

A CDR consumer is different from a 'consumer' as used in the other parts of the *CCA* and it includes businesses,[61] as the rights to share data are exercisable by businesses as well as consumers.[62] This can be seen from the privacy safeguards set out in the CCA,

55. *Id.* s 56BC(1)(c).

56. *Id*. ss 56BB(d), 56BH.

57. *Id.* s 56BC(2).

58. *Id.*

59. *Id.* s 56BC(3).

60. *Id.*.

61. *Id*. s 56AI. This definition does not apply to subsection 4(1) of the *CCA,* which defines 'consumer' for the general purposes of the Act. *Id.*; The breadth of protection of the CDR is in contrast to the regulatory protection offered by the ePayments Code in Australia, which does not apply to business accounts. ePayments Code 2016 (Cth) ch A (Austl.).

62. There is flexibility in the legislative structure to change the definition of CDR consumer for different sectors. Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) ¶ 1.112 (Austl.).

which protect the privacy or confidentiality of CDR consumers' CDR data, whether the consumers are individuals or corporate bodies.[63] These safeguards apply primarily to accredited data recipients in place of the Australian Privacy Principles ('APPs') under the *Privacy Act 1988* (Cth) ('Privacy Act').[64] The APPs continue to apply to data holders as most of the privacy safeguards do not apply to them.[65] The privacy safeguards have equivalent scope as the APPs, covering the collection of data,[66] the use or disclosure of data,[67] and the security, destruction and de-identification of data.[68] However, unlike the APPs, the safeguards also apply to businesses that are CDR consumers.[69] These obligations are supported by the Australian Standards.[70]

(b) Foundation of Legal Responsibilities Under UK Open Banking

Open banking in the UK was established to address a competition problem in the retail banking market identified by the UK Competition and Markets Authority ('CMA'),[71] and also to implement the EU's *Revised Payment Services Directive* ('*PSD2*').[72] The PSD2 is intended to continue the development of an integrated internal market for safe electronic payments, in part to ensure 'that consumers, merchants and companies enjoy choice and transparency of payment services.'[73] Accordingly, two separate legislative instruments form the legal foundation of UK open banking: part 2 of the *Retail Banking Market Investigation Order 2017* (UK) ('*CMA Order*')[74] of the CMA, and part 7 of the *Payment Services Regulation 2017* (UK) ('*PSR*'),[75] which translated *PSD2* into UK legislation.[76]

63. *Competition and Consumer Act 2010* (Cth.) s 56EA (Austl.).

64. *Id.* s 56EC(4)(a); *See Privacy Act 1988* (Cth) (Austl.).

65. Only the privacy safeguards relating to open and transparent management of CDR data, notification of the disclosure of CDR data, quality of CDR data, and correction of CDR data apply to data holders. *Competition and Consumer Act 2010* (Cth.) ss 56ED, 56EM, 56EN, 56EP (Austl.).

66. *See id.* s 56EF.

67. *Id*. s 56EI.

68. *Id.* s 56EO.

69. *See* James Meese et al., *Citizen or Consumer?: Contrasting Australia and Europe's Data Protection Policies*, 8(2) INTERNET POL'Y REV., June 30, 2019, at 2, 6.

70. The *CCA* provides for the Australian Standards to cover the "collection, use, accuracy, storage, security and deletion of CDR data." *Competition and Consumer Act 2010* (Cth.) s 56BB (Austl.).

71. *See* Press Release, Competition and Mkts. Auth., *supra* note 41; DIXON, *supra* note 32, at 189.

72. *See PSD2*, *supra* note 7, ¶ 2.

73. *Id.* ¶ 5.

74. COMPETITION AND MARKETS AUTHORITY, THE RETAIL BANKING MARKET INVESTIGATION ORDER (2017) [hereinafter CMA ORDER]. The *CMA Order* is made under the Enterprise Act. The Enterprise Act 2002, c. 40 (U.K.).

75. The Payment Services Regulations 2017, SI 2017/752 (UK).

76. The Payment Services Regulations 2017, Explanatory Memorandum ¶ 7.4 (U.K.).

The *Retail Banking Market Investigation Order 2017* ('*CMA Order*')[77] of the UK Competition and Markets Authority ('CMA'), provides very limited detail on the responsibilities for shared data. It requires that the Read/Write Data Standard contains security standards for compliance by data recipients,[78] and the *Explanatory Note* to the *CMA Order* provides that the Open Banking Implementation Entity ('OBIE') 'will ensure that customers are fully protected against privacy and security risks.'[79] However, no further clarity is provided, other than that it needs to consider the *General Data Protection Regulation ('GDPR')* of the European Union ('EU').[80]

The *Payment Services Regulation 2017* (UK) ('*PSR*')[81] contains substantive legal responsibilities on Account Information Service Providers ('AISPs').[82] These relate to the use of the shared data, the requirements for consent, and the storage of the shared data.[83] They are supported by the standards ('UK Standards') produced by the OBIE in accordance with the *CMA Order*.[84] Unlike Australian open banking, UK open banking does not contain its own privacy or data protection regime for shared open banking data. Accordingly, when it was established, the UK framework relied on *GDPR* to apply to customer data shared with an AISP which is 'personal data' for the purpose of *GDPR*.[85] The *GDPR* applies to customer data in the UK framework which is 'personal data,' being information relating to an identified or identifiable natural person.[86]

77. CMA ORDER, *supra* note 74.

78. *Id.*

79. Retail Banking Market Investigation Order 2017, Explanatory Note ¶ 38 (U.K.).

80. *Id.*; GDPR, *supra* note 17.

81. The Payment Services Regulations 2017, SI 2017/752 (UK).

82. *Id.* art. 17-21, art. 60, art. 70(3). An Account Information Service Provider is defined by reference to the provision of an account information service. *Id.* art. 2, ¶ 1; *See infra* Part II.1(a).

83. The Payment Services Regulations 2017, SI 2017/752, art. 70, ¶ 1-3 (UK).

84. The "Customer Experience Guidelines" cover the provision of the consent of the consumer to the use of the transferred data. *See Customer Experience Guidelines*, OPEN BANKING, https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/ (last visited Feb. 7, 2022).

85. For the need to comply with both *PSR* and *GDPR* see FIN. CONDUCT AUTH., PAYMENT SERVICES AND ELECTRONIC MONEY – OUR APPROACH 91, 95 (2017); The connection between *GDPR* and *PSD2* is recognised in *PSD2*. *PSD2*, *supra* note 7, at recital 89, art. 94(1); Although *PSR* contains neither that recital, nor that wording, it is clear that *GDPR* still applies to the personal data held under the UK framework because following the withdrawal of the UK from the EU, the *GDPR* effectively became part of the domestic law of the UK and the effect was to create a 'UK *GDPR*' as defined in the *EU Exit Regulations*. *See* European Withdrawal Act 2018, c. 16, § 3 (UK); Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No 2) Regulations 2019, SI 2019/0000, sch. 1 (UK). However, for simplicity this article will continue to refer to it as the *GDPR*.

86. Including someone who can be directly or indirectly identified by reference to an identifier, such as a name or identification number. *GDPR*, *supra* note 17, at art. 4(1).

The following parts of this article build upon this foundation by comparing the legal responsibilities of data recipients under the Australian and UK open banking frameworks and evaluating them against a bank's responsibilities for custody of funds received for a customer under banking law. The legal responsibilities analysed as those in requesting customer data (Part 3), in using shared customer data (Part 4), for the integrity of shared customer data (Part 5), and in authorization to receive customer data (Part 6).

III. Legal Responsibilities in Requesting Customer Data

A central foundation of the accountability of data recipients under open banking in Australia and the UK is the data minimization principle. Based on one of the six core principles of processing personal data under *GDPR*,[87] it limits the data which can be shared to those which are necessary to achieve the purpose of sharing the data. In the US, the relevance of data minimization has been recognised in the discussions already conducted with the CFPB.[88] Responsibilities relating to data minimization under Australian and UK open banking are comparatively analysed below, followed by evaluation against responsibilities of banks in receiving customer funds under banking law.

1. Comparison of Data Minimization in Australian and UK Open Banking

(a) Scope of Data Minimization

Data minimization is incorporated into the Australian framework through the *CDR Rules*.[89] It prohibits an accredited person from using CDR data beyond what is reasonably required to provide goods or services which have been requested by the customer.[90] It is supported by a separate requirement in the *CDR Rules* that an accredited person can only request CDR data needed to provide those goods or services.[91] For example, an accredited person must not request ongoing access to transaction data in order to assess eligibility for loans at a single point in time, and

87. *Id.* art. 5(2); The others are the principles of: lawfulness, fairness and transparency; purpose limitation; accuracy; storage limitation; integrity and confidentiality. *Id*. art. 5(1)(a), (b), (d)-(f).

88. *See* Consumer Access to Financial Records, *supra* note 22; CONSUMER FIN. PROT. BUREAU, BUREAU SYMPOSIUM: CONSUMER ACCESS TO FINANCIAL RECORDS, 6 (2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

89. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) reg 1.8 (Austl.).

90. *Id.* regs 1.8, 4.4.2.

91. *Id.* at reg 4.3(1).

must not use data supplied for the provision of an account aggregation service to create a profile of customers' spending habits.[92]

The *PSR* incorporates a conceptually similar limitation into the UK framework. An AISP must not use, access, or store any information except for the purpose of the account information service ('AIS') explicitly requested by the payment service user.[93] The AIS is

> *'[a]n online service to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or with more than one payment service provider, and includes such a service whether information is provided-*
>
> *(a) in its original form or after processing;*
>
> *(b) only to the payment service user or to the payment service user and to another person in accordance with the payment service user's instructions.'*[94]

An AISP is not permitted to use data shared with it under the *PSR* for the provision of services other than an AIS. As a result, the scope of the data use permitted in the UK framework initially appears very narrow and would not permit use for purposes such as assessing credit or completing loan applications. However, flexibility is provided through the inclusion in the definition of AIS of the ability to provide the consolidated information to another person, in addition to the customer, on the customer's instructions. This other person could be, for example, a third party that provides credit scoring services and makes loan applications.[95]

These requirements of the *PSR* are complemented by the data minimization principle in *GDPR* which applies to personal data shared using UK open banking. This means that a data recipient under UK open banking must not collect personal data beyond those required to supply the specific AIS requested by the customer and access to the personal data should be limited to what is necessary for that purpose.[96] For example, an AISP is not permitted to process the description of

92. Explanatory Statement, Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) regs 10-11 (Austl.).

93. The Payment Services Regulations 2017, SI 2017/752 art. 70 ¶ 3(f) (UK).

94. *Id*. at reg 2(1) (defining "acount information service").

95. *See AISP Models under PSD2*, FIN. CONDUCT AUTH. (Jan. 21, 2020), https://www.fca.org.uk/firms/agency-models-under-psd2.

96. Eur. Data Prot. Bd., G*uidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR*, at 21 (Dec. 15, 2020).

transactions in open banking data if it is not necessary for the account information service which the AISP provides.[97]

The primary difference in data minimization between the two frameworks is in their scope. Australian open banking requires that the data is needed for a good or service requested by the customer,[98] but there is no limit on the good or service which may be requested. This contrasts with UK open banking where the service requested by the customer must be an account information service.[99] As the ability to share data is essential to the data portability function of open banking,[100] the narrowness of the permitted service could limit the benefit of UK open banking. However, as noted above, there is further flexibility through the ability to provide the consolidated account information to a third party which can enable other services to be provided.[101] In these circumstances, the requirements of *GDPR*, including its less restrictive data minimization principle, would apply to the third party.[102] This should enable a similar breadth of potential uses to be requested by the customer under UK open banking as are available in Australia. Accordingly, with the appropriate use of third parties, the design of UK open banking with respect to data minimization should not significantly reduce the data which a customer may share in comparison to Australian open banking. The need to use those third parties to achieve this could itself be regarded as an unnecessary source of complexity but this should be able to be managed through agency and outsourcing arrangements by data recipients.

(b) Effect of Data Minimization on Data Sharing Relationships

The incorporation of data minimization into open banking shapes the nature of the relationship between customer and data recipient.[103] The data that is shared is

97. *Id.* at 22.

98. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) reg 1.8 (Austl.).

99. The Payment Services Regulations 2017, SI 2017/752 art. 70 ¶ 1-3 (UK).

100. *See supra* Part III.1.A.

101. *See supra* text accompanying note 95.

102. *See AISP Models under PSD2*, *supra* note 95.

103. Under the UK framework this transaction is required to be established in a contract between the customer and the data recipient for the account information service: 'Payment services [under *PSD2*] are provided on a contractual basis between the payment services user and the payment services provider': Eur. Data Prot. Bd., *supra* note 96, at 9; *See PSD2, supra* note 7, at recital 87; There is no similar requirement for a pre-existing contract specified in the legislative instruments of the Australian framework, although the *CDR Rules* do refer to the 'relevant contract' between the accredited person and the CDR consumer relating to the requested supply in its provisions for revocation or suspension of a person's accreditation. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) reg 4.17 (Austl.). However, the foundations of contract formation should be present if the customer has requested the supply of the good or service and the data recipient has agreed to provide it in exchange for the receipt of the customer's data, assuming contractual capacity is present.

more than something of value exchanged by the customer in return for the good or service. Instead, it is an essential requirement which the customer contributes for the provision of the good or service which they have requested. Because of data minimization, customers in open banking do not share their data to 'purchase' the supply which they have requested.[104] This differs from other data sharing arrangements where the customer receives a 'free' service in exchange for their data, which the recipient uses to gain knowledge about the customer's preferences and behaviour for their own economic gain.[105] By confining the data shared to what is needed, data minimization seeks to balance the exchange between customer and data recipient.[106] This relationship, enabled by data minimization, balances the portability and accountability functions of open banking frameworks by constraining the data shared to what is needed for their use. In this regard, the differences between the frameworks identified above are not as relevant as they do not affect the need for the data requested to be linked to its use. However, to evaluate this further, it is necessary to compare it with the use of customer funds by the customer's bank.

2. Evaluation Against Bank's Responsibilities in Use of Customer Funds

(a) No Similar Limits on Use of Customer Funds

Banking law does not incorporate obligations equivalent to data minimization in relation to customer funds. There is no legal requirement that a bank may only apply funds received on behalf of its customer to the extent needed for the bank to provide another service which has been requested by the customer. Instead, once money is credited to the customer's account by the bank, it 'is then the banker's money; he is known to deal with it as his own; he makes what profit of it he can, which profit he retains himself.'[107] In taking custody of its customers' funds, the bank offers its customers the benefits of storage and liquidity by agreeing to repay the amount received at the customer's request.[108] It is possible for this to be

104. *See* Directive 2019/770, of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, 2019 O.J. (L 136) 1.

105. *See* Santiago Ramirez Lopez, *Informing Consent*, 9 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 35, 47 (2018); This circumstance can arise because the incremental value of another person's data to a firm which has 'accumulated a critical mass of consumer data' are small so that the consumer's 'best deal is to exchange their personal data in return for a free online service that has a higher marginal use value for them than the depressed market value of their individual data.' Martens, *supra* note 19, at 8; *See also* Malgieri & Custers, *supra* note 37, at 11.

106. *See* ROBERT WALTERS ET AL., *DATA PROTECTION LAW: A COMPARATIVE ANALYSIS OF ASIA-PACIFIC AND EUROPEAN APPROACHES* 53-55 (2019) (noting that re-balancing the relationship between data subject and data controller is also part of the aim of data portability under the GDPR).

107. *See* Foley v. Hill (1848) 9 Eng. Rep. 1002 (HL) 1005-06 (UK).

108. *See* Awrey & Zwieten, *supra* note 29, at 800.

provided in connection with another service requested by the customer, such as the custody of the customer's securities or the safekeeping of the customer's other valuable property. But, the bank's responsibilities for the customer's funds are not dependent on, and the bank's rights to use the funds received are not limited by, any such additional service. Accordingly, data minimization represents a significant difference between open banking laws and banking laws.

There would be a significant adverse impact on the effectiveness of the banking if data minimization were to apply to funds received for a customer by their bank. It would mean that a bank could only use those funds to the extent they are needed to provide another service which the customer had requested. This might arise in some circumstances, for example if the funds are needed as collateral for financing made available for the customer. However, it would not arise where the customer just wanted to keep their funds at their bank. Accordingly, key benefits provided by the banks, like the bank being able to on-lend the funds as its own and the customer not having to hold and use cash, would be severely constrained.

Nevertheless, before seeking to derive any conclusion from this in relation to the inclusion of data minimization in open banking, it is necessary to analyse whether there are relevant differences in customer data and customer funds. One particular feature of customer data is important, namely that the value of customer data depends on their use, whilst the value of customer funds do not.

(b) Use-Dependency of the Value of Customer Data

Data is not inherently valuable, and value is derived from data through use: 'Data value is derived not by *what data is*, but by *what can be done to create value* with data.'[109] Customer data produces value for the customer when it is used for the customer's benefit and different uses of the same data produce different value.[110] For example, a customer's banking data produces more value for a customer when it is used to move the customer's money to the account which, at that time, is paying the highest interest rate than when used to inform a customer of their account balance. This dependency of value on use does not apply to customer funds. Due to money's functions as a store of value and a unit of account,[111] customer funds in a bank account maintain their value whilst they are stored and when being used.

This difference challenges the argument that data minimization imposes a constraint on the effectiveness of open banking. Data minimization means that a

109. Peter Leonard*, Is Data Your Most Valuable Asset that You Never Owned?*, DATA SYNERGIES 1 (Aug. 2018), https://www.iot.org.au/wp/wp-content/uploads/2016/12/Peter-Leonard-Is-Data-Your-Best-Asset-You-Never-Owned-23-August-2018.pdf; LUCIANO FLORIDI, INFORMATION: A VERY SHORT INTRODUCTION 97 (2010).

110. *See* Reimsbach-Kounatze, *supra* note 17, at 72.

111. *See* PROCTOR ET AL., *supra* note 32, at ¶ 1.31; FOX, *supra* note 32, at ¶ 1.38; BRINDLE & COX, *supra* note 35, at ¶ 3-002.

customer exchanges data in return for a good or service from the data recipient which requires those data. For the exchange between the customer and data recipient to be fair, both customer and data recipient need to understand the value of what they are exchanging.[112] If the customer does not understand the use to which their data is to be put, then the customer cannot understand the value of what they are providing, or the 'price' which they are paying.[113] However, the data recipient is not in the same position as they know the use to which they intend to put the customer's data. This information asymmetry as to the use of the customer's data creates an imbalance between customer and data recipient, and potential unfairness in the data exchange. A similar balance would arise in banking if a bank were able to choose the term and interest rate for the investment of a customer's funds in a term deposit without having to inform, or consult with, the customer.[114]

The incorporation of data minimization in the open banking frameworks addresses this asymmetry in the relationship between the customer and data recipient by requiring that the data can only be used for the purpose of providing the good or service which the customer has requested. This results in the use of the shared data being in accordance with the customer's direction. Accordingly, data minimization should not be considered a flaw in the design of open banking when compared to banking, but a feature which is intended to improve the fairness of the data sharing.

However, its ability to achieve that fairness is dependent on the data recipient complying with its data minimization responsibilities. Similar reliance on data controller compliance has been identified as a weakness in data protection regimes.[115] This is not solely because of willing non-compliance with obligations. Data-related rules are often difficult to comprehend due to their complexity, and difficult to apply in practice because they are often not 'workable, sector-specific, and context-specific.'[116] Of particular concern is the potential for customer data transferred under open banking to be commingled with data which is not subject

112. VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA 41 (2018) ("[T]he overwhelming view among economists is that in markets, more information trumps less.").

113. Malgieri & Custers, *supra* note 37, at 289 ("[I]f individuals are shown the 'price' of their personal data, they can acquire higher awareness about their power in the digital market and thus be effectively empowered for the protection of their information privacy.").

114. Although this example is hypothetical, a related issue was identified to be of concern by the Australian Securities and Investments Commission (ASIC) in relation to the renewal of maturing term deposits with Australian banks at lower interest rates with insufficient disclosure or opportunity for the customer to prevent the renewal. *See* AUSTL. SEC. & INV. COMM'N, REVIEW OF TERM DEPOSITS 26 (2010).

115. *See* Bert-Jaaps Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIV. L. 250, 253-54 (2014).

116. *Id*. at 254. Further, compliance often takes the form of ensuring that tasks on a checklist are completed for the purpose of showing supervisors and auditors, rather than achieving the purpose of the regulation. *Id.*; Neil Robinson et al., *Review of the European Data Protection Directive*, RAND Europe (May 2009).

to the same obligations such that it becomes impossible to comply with the open banking responsibilities. The design of each framework manages this to some extent by allowing for the responsibilities under the respective data protection regimes to apply in place of those under open banking. For example, under Australian open banking, an authorised deposit-taking institution ('ADI') that receives data under the Australian framework is treated as a data holder and not a data recipient for that data if the customer has acquired a product from them, the ADI reasonably believes that the data is relevant to the product and has obtained the customer's consent.[117] This reduces the complexity in managing the transferred data because the data, and the other data held by the ADI in respect of that customer and product, becomes subject to the APPs of the *Privacy Act* instead of many of the privacy safeguards under the *CCA.*[118] A similar effect is achieved under the UK framework, in that *GDPR* and not the *PSR* applies to the treatment of the consolidated account information which is provided to a third party.[119]

These mechanisms are not perfect and will not remove all potential difficulty in complying with responsibilities for transferred data in the context of holding large amounts of customer data from different sources. Also, they will not remove the risk that a data recipient does not comply with its obligations even though it could. These risks apply also to the use of customer's consent in each framework and are analysed further in that context in Part 4 below.[120]

3. Summary

The above analysis shows that although the data minimization is framed differently in Australian and UK open banking, in practice the difference should not be meaningful for effectiveness in performing their accountability function. It has also shown that data minimization imposes a limitation on the use of customer data which, if it were imposed similarly on customer funds, would reduce the benefit for customers and banks in banking payments. However, this difference should not be considered a flaw in open banking's design as it results from a difference in the nature of customer data and customer funds, namely that the value of customer data is determined by its use. Accordingly, instead of causing the same loss of benefit in the frameworks, data minimization improves the effectiveness of the

117. *Competition and Consumer Act of 2010* (Cth) sub-div 56AJ(4) (Austl.); *CDR Rules*, *supra* note 6, r 7.2.

118. *Id.* at sub-divs 56ED, 56EM, 56EN, 56EP. However, it is unclear why this should be limited to ADIs as other data recipients. For example, accounting platforms could also be disadvantaged by the need to treat comingled data separately.

119. *See AISP Models under PSD2*, *supra* note 95 and accompanying text.

120. Data minimization and consent are not alternatives, both are required. This is more complicated for the purpose of applying the *GDPR* because consent under *PSD2* is not recognised as the consent needed to process information under *GDPR*: Eur. Data Prot. Bd., *supra* note 96. However, this is not relevant to this analysis.

exchange between customer and data recipient by addressing the information asymmetry which would otherwise be present relating to how the customer's data are to be used. Nevertheless, the effectiveness of data minimization relies on the performance of the data recipient of its legal responsibilities and customers are exposed to risk of non-performance. This also applies to the legal responsibilities in using shared customer data.

IV. LEGAL RESPONSIBILITIES IN USING SHARED CUSTOMER DATA

Consent is at the foundation of data sharing.[121] The need for a customer's consent is incorporated into Australian and UK open banking as it is critical to the customer autonomy and recipient accountability. For example, in Australia

> *[c]onsumer consent for the collection and use of their data is the bedrock of the CDR regime. Consent enables consumers to be the decision makers in the CDR regime, ensuring that they can direct where their data goes in order to obtain the most value from it.*[122]

Consent has already played an important role in the discussions conducted with the CFPB,[123] and informed consent was one of the nine principles articulated by the CFPB in their 2017 Principles.[124] The responsibilities relating to two aspects of consent, its nature, and criticisms of reliance on it, under Australian and UK open banking are comparatively analysed below, followed by evaluation against control of the use of funds and the value of what is transferred in banking payments.

1. Comparison of the Role of Consent in the Open Banking Frameworks

(a) Each framework requires express, clear, and specific consent

Australian and UK open banking both rely on customer consent to authorise and control the use of customer data. Neither of the frameworks provides an alternative basis on which a data recipient may obtain or use customer data. This

121. *See* Fracassi & Magnuson, *supra* note 19.

122. *Chapter C: Consent — The basis for collecting, using and disclosing CDR data*, OAIC (June 2021), https://www.oaic.gov.au/__data/assets/pdf_file/0023/7475/chapter-c-consent-final.pdf.

123. *See* Consumer Access to Financial Records, 85 Fed. Reg. 71003 (proposed Nov. 6, 2020); CONSUMER FIN. PROT. BUREAU, *supra* note 88.

124. CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED DATA SHARING AND AGGREGATION (OCT. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

differs from each jurisdiction's respective data protection laws, *GDPR* and the *Privacy Act*, which provide other bases on which data may be used.[125]

The privacy safeguards in the *CCA* provide that CDR data may not be used by an accredited person unless the use is authorised under the *CDR Rules.*[126] The *CDR Rules* permit the data to be used if it is in accordance with both the data minimization principle, and current consent of the customer.[127] Further permitted uses include deriving data from the data for that same purpose and de-identifying the data for general research or disclosure (with consent) and disclosure to specified support providers.[128]

Similarly, the *PSR* relies on consent. It requires that the AISP that receives data of a payment service user:

- not provide account information services without the payment service user's explicit consent, and
- not use, access, or store any information for any purpose except for the provision of the account information service explicitly requested by the payment service user.[129]

Further, the *PSR* requires that an AISP must not access, process, or retain any personal data for the provision of payment services by it, unless it has the explicit consent of the payment services user to do so.[130]

The *CDR Rules* require that consent be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[131] They further require that the consent:

125. Under *GDPR* contractual necessity, legal compliance, protection of vital interests, public interest and legitimate interests are also lawful bases for the processing of personal information. *See* Commission Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36-37 (EU). Under the *Privacy Act* personal information can be collected if the information is reasonably necessary for one or more of the entity's functions or activities and used for the purpose for which it was collected, or a secondary purpose which is related to it, if such a use would be reasonably expected. *See Privacy Act 1988* (Cth) sch 1 cls 3, 6 (Austl.).

126. *Competition and Consumer Act of 2010* (Cth) sub-div 56EI(1)(b) (Austl.).

127. *Competition and Consumer Rules 2020* (Cth) r 7.5 (Austl.); Neither the *CCA* nor the *CDR Rules* define 'use'. The Australian Office of the Information Commissioner has defined an entity to use CDR data when it 'handles and manages that data within its effective control', for example by accessing, reading and searching the data, making a decision base on it, passing it from one part of the entity to another, deriving data from it or de-identifying the data. Off. of the Austl. Info. Comm'r., *supra* note 122, at ¶ B.149.

128. *Competition and Consumer Rules 2020* (Cth) r 7.5 (Austl.); There are specific restrictions on the use of the CDR data for direct marketing. *Id.*; *see infra* Part IV.1.b pp. 322-326.

129. The Payment Services Regulations 2017, SI 2017/752, art. 70, ¶ 7 (UK).

130. *Id*. reg. 97.

131. *Competition and Consumer Rules 2020* (Cth) r 4.9 (Austl.).

- be obtained in accordance with the CDR data standards, including the consumer experience standards, and have regard to the consumer experience guidelines,[132]
- not include or refer to other documents so as to reduce comprehensibility or be bundled with other directions, permissions, consents, or agreements,[133]
- enable the customer to choose the types of CDR data to which the consent applies and the specific uses to which they are consenting,[134] and
- allow the customer to choose whether the consent applies to a single occasion or over a specified period of time.[135]

A consent expires if it is withdrawn, its period has expired or 12 months has passed since it was given.[136] Further, an accredited person must only seek a consent in compliance with the data minimization principle and must not seek a consent for the purpose of identifying, compiling insights on, or building a profile in relation to, any identifiable person who is not the CDR consumer who made the consumer data request.[137]

The requirements for consent under the UK framework are similar. As noted in paragraph (a) above, the consent is required to be 'explicit'.[138] In the view of the Financial Conduct Authority ('FCA'), explicit consent under the *PSR* requires that the AISP

> *should make available to customers the information needed to make an informed decision and understand what they are consenting to (e.g., they must be able to understand the nature of the service being provided to them) and the consent should be clear and specific. For AISPs, aside from any requirements of data protection legislation, we consider this to include information about how the customer's payment account information will be used and whether any other parties will have access to that information.*[139]

132. *Id.* at r 4.10.
133. *Id*.
134. *Id.* at r 4.11.
135. *Id*.
136. *Id*. r 4.14.
137. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.12 (Austl.).
138. The Payment Services Regulations 2017, SI 2017/752, art. 70, ¶ 3 (UK).
139. FIN. CONDUCT AUTH., *supra* note 85, at 212.

This means, for example, that the customer's consent must be obtained for any analytics to be performed on the information as part of an account information service.[140] This use of the phrase 'explicit consent' causes some complication in the UK framework because it does not have the same meaning as it does in *GDPR*.[141] In fact, under *GDPR*, the processing of personal data under the UK open banking framework is not authorised on the basis of consent, but on the basis of it being 'necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.'[142] This requires that an AISP needs to be able to demonstrate that the data being used is objectively necessary for its provision of the account information service.[143] It also requires that the contract with the payment service users makes them fully aware of the specific categories of data that will be used and the purpose to which they will be put.[144]

The standards under each framework provide further guidance on the form of consent. The Australian Standards require that the consent process should be easy to understand, each customer must be presented with an active choice to give consent, consent should be a genuine choice and should not be a precondition of service.[145] Further, for the purpose of understanding consents, statements as to the purpose and use of data should be specific, refer to the broader uses and relate to the goods or services provided.[146] Similarly, the UK Standards provide that 'an AISP must make it very clear why it's needed, what's being shared and for how long.'[147] This includes language for purpose statements, provision of enough information to make informed decisions, and use of the recommended structure and language.[148]

This shows that the requirement for, and the requirements for the form of, consent are similar in each framework. Consent is needed under both frameworks,

140. *See* UK FINANCE, PSD2 GUIDANCE: OPEN ACCESS – GUIDANCE FOR TPPS 7 (2020), https://www.ukfinance.org.uk/system/files/PSD2%20Guidance%20Section%201%20Open%20Access%20Guidance%20ASPSPs%20January%202020%20-%20updated%20July%202020.pdf.

141. *See* Eur. Data Prot. Bd., *supra* note 96, at 14; Commission Regulation 2016/679, art. 9, 2016 O.J. (L 119) 38 (EU) (explaining that explicit consent is required under GDPR only for "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership" as well as "data concerning health or data concerning a natural person's sex life or sexual orientation," or genetic or biometric data).

142. Eur. Data Prot. Bd., *supra* note 96, at 8; Commission Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36 (EU).

143. Eur. Data Prot. Bd., *supra* note 96, at 9.

144. *Id.* at 13.

145. CONSUMER DATA STANDARDS, *Consumer Experience Guidelines*, v 1.16.1, https://consumerdatastandardsaustralia.github.io/standards/#introduction (last visited Feb. 2, 2022).

146. *Id*.

147. *Customer Experience Guidelines*, OPEN BANKING, https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/customer-journey/latest/ (last visited Feb. 2, 2022).

148. *Id*.

and must be voluntary, express, specific, informed, and clear – more so than under the respective data protection regimes.[149] This enhances the effectiveness of both frameworks in performing their custody function by ensuring that the data shared is appropriately used.

However, the reliance on consent by those data protection regimes is subject to criticism, which needs to be analysed in the context of the open banking frameworks.

(b) Criticisms of Reliance on Consent

In the context of data protection and privacy law, consent has been criticised as a method of authorizing the processing of personal information and providing control to data subjects.[150] The reasons for this criticism include that the large quantity of information given to a person in order to obtain their informed consent places too much of a cognitive load on them for the consent to be truly informed.[151] It is often given on a 'non-negotiable, non-informed, and pressurized basis' which makes it 'an illusion,'[152] with the result that consent is 'largely theoretical and has no practical meaning,'[153] and the principle of 'privacy self-management' on which consent rests is 'a vast, complex, and never-ending project that does not scale' with the result that the 'best people can do is manage their privacy haphazardly.'[154]

The design of Australian and UK open banking seeks to manage these shortcomings of consent through two features:

- *Standardisation:* each framework seeks to standardize the consent process through the application of customer experience standards and guidelines based on consumer experience testing.[155] These are intended to create a consistent experience for customers in providing their consent, so that the process can become familiar regardless of the data recipient with whom they are dealing, and so that consent fatigue

149. Commission Regulation 2016/679, art. 9, 2016 O.J. (L 119) 38 (EU) (noting that implied consent is permitted under the *Privacy Act 1998* (Cth) (Austl.) s 6(1) and explicit consent is required only for particular types of personal data); *see supra* note 141 above and accompanying text.

150. *See* Koops, *supra* note 115; Fracassi & Magnuson, *supra* note 19, at 374 ("It is remarkably easy to get consumers to consent to anything on the internet.").

151. *See* Yoan Hermstruwer, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent And Big Data*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 9, 18 (2017); Lopez, *supra* note 105, at 46.

152. *Id.* at 39.

153. Koops, *supra* note 115, at 251.

154. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 5 (2020).

155. CONSUMER DATA STANDARDS, *Consumer Experience Guidelines*, v 1.16.1, https://consumerdatastandardsaustralia.github.io/standards/#consent-standards (Australian Consumer Data Standards) (last visited Apr. 18, 2022); *See Customer Experience Guidelines*, *supra* note 147 (UK Data Customer Journey).

can be reduced. This standardization includes language used in describing the data which can be used and allocation of the data into 'clusters' which can be grouped together for better comprehension.[156] This standardization be taken further in Australian open banking, with the creation of a 'CDR dictionary' so that particular words to have standardized meanings and for those words to be drafted in a 'formulaic way' so that they could be more readily codified for use with data technologies.[157] Codification of consent so that it can be attached to data has also been recommended for the UK framework.[158]

- *Consent management:* each framework provides access to customers to the consents which they have provided, so that they can be understood, managed, and withdrawn. Consumer 'dashboards' are required under both the Australian Standards and the UK Standards,[159] although in UK open banking (unlike Australian open banking) they need only be provided by the bank and not the data recipient.[160] This concept should be taken further in Australia to enable centralised consent management services to be offered to customers by providing for the customer's consents themselves to be sharable under the Australian framework.[161]

It is too early to assess if these strategies for the management of the shortcomings of consent will be successful. A lot depends on the technologies being both effective and easily used by customers. If they are not successful, customers could become overwhelmed with the complexity of having to understand and

156. "OBIE customer research found that grouping permissions together and adding another layer of description aided the PSU's understanding of the data they were being asked to consent to share. This approach also allows a consistency of language across AISPs and ASPSPs to provide additional comfort to PSUs that they are sharing the data they intended to. If consistent language is used across all Participants this will drive PSU familiarity and adoption." *See Permissions & Data Clusters for AIS journeys*, OPEN BANKING, https://standards.openbanking.org.uk/customer-experience-guidelines/account-information-services/permissions-and-data-clusters/latest/#:~:text=In%20the%20Open%20Banking%20API,data%20elements%20in%20the%20permission (last visited Apr. 18, 2022).

157. COMMONWEALTH TREASURY, *supra* note 42, at 133-34.

158. OPEN DATA INSTITUTE & FINGLETON, OPEN BANKING, PREPARING FOR LIFT OFF 5, 37 (2019), https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

159. *Consumer Experience Guidelines*, CONSUMER DATA STANDARDS v. 1.4.0 (2020), https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/08/CX-Guidelines_v1.4.0.pdf (noting the guidelines for consumer data in Australia); *See AIS Access Dashboard & Revocation*, *supra* note 147 (discussing the UK Open Banking Standards).

160. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) rr 1.14-1.15 (Austl.).

161. COMMONWEALTH TREASURY, *supra* note 42, at 142.

manage the consents which they have provided for the use of their data. Following the analysis above, this would reduce the customers' ability to understand how their data is used, the value of the data which they are sharing and, as a result, the 'price' which they are paying for the goods or services which they have requested. This would render the sharing of data less beneficial and less safe for customers and cause the reliance on consent to challenge rather than support the recipient accountability in open banking. Nevertheless, the reliance on consent needs to be evaluated against customers' rights in controlling their funds.

2. Evaluation Against Customer Rights in Controlling Customer Funds

(a) No Customer Control Over Bank's Use of Funds

As analysed in Part 3.2, a customer does not control their bank's use of the funds received by the bank on the customer's behalf. Although a bank receives a funds transfer as its customer's agent, this does not grant control of the funds to the customer because the bank's authority in that agency is limited to receiving the payment and crediting the payment to the customer's account.[162] Once the funds are credited to the customer's account, the funds are owned by the bank as principal, not as trustee or agent, and the bank owes a debt to the customer for the amount credited to the customer's account.[163] The bank

> *is not bound to keep it or deal with it as the property of the customer, but he is, of course, answerable for the amount, because he has contracted, having received that money, to repay to the customer, when demanded, a sum equivalent to that paid into his hands.*[164]

The right to repayment of that 'sum equivalent' represents the 'money' of the customer comprised in the balance of their bank account and the bank's responsibilities to its customer for the transferred funds are encompassed in its promise to repay that amount. The funds actually 'received' belong to the bank, may be dealt with by the bank as its own funds, and are not subject to the

162. *See* GEVA, *supra* note 28 at 294 (citing Royal Products Ltd v. Midland Bank Ltd [1981] 2 Lloyd's Rep. 194); The Laconia [1976] 2 All ER 249; For Australia, *ANZ Banking Group v Westpac Banking Corporation* (1988) 164 CLR 662 (Austl.). Geva notes that 'it is not universally accepted that the beneficiary's bank acts as the beneficiary's agent' and instead it has been argued that the beneficiary's bank as sub-agent of the payer: GEVA, *supra* note 28 at 295. However, he concludes that '[t]he act of payment to the customer by the beneficiary's bank is thus under the contract with the customer, more than in fulfilment of the sender's instructions, so that the beneficiary's bank ought to be regarded as acting throughout as an agent for the beneficiary': *Id.*

163. *See Joachimson v. Swiss Bank Corp.* [1921] 3 KB 110 (U.K.); Foley v. Hill (1848) 9 Eng. Rep. 1002 (HL) 1005-06 (UK); The principal from these cases that the primary relationship between banker and customer is that of debtor and creditor was approved in Australia in *Laing v Bank of NSW* (1952) 69 WN (NSW) 318 (N.S.W.).

164. *Foley*, 9 Eng. Rep. at 1006.

customer's control or consent.[165] This enables the bank to on-lend those funds, creating credit and generating value and benefit in the banking system.[166]

This means that the requirement for consent represents a significant difference between open banking and banking. If a data recipient had the same freedom to use customer data as the bank does to use customer funds, then open banking would be more like 'open data' arrangements, where the data 'is accessible to anyone, published under a license that allows people to use, share and modify it for any purpose.'[167] Neither Australian or UK open banking takes this approach and each only allows data to be shared when authorised by the customer.

Just as with data minimization, there would be a significant adverse impact on the benefits provided by banking if a bank required the consent of its customer to use the funds which it receives for the customer. The bank could no longer lend or otherwise invest those funds as it chose and the bank's ability to create credit and generate gains using those funds, would be limited. It would also change the nature of the bank's business by placing the management of its assets into the control of individual customers. In doing so, it would likely threaten the bank's viability as its functions of liquidity transformation, maturity transformation and credit transformation need to be managed on a portfolio basis rather than on an individual asset and liability basis.[168]

This would seem to support the argument that, when evaluated against banking, the requirement for consent in open banking is a constraint on its effectiveness and, as a result, a flaw in its design. However, just as with data minimization, it is necessary to analyse whether there is a relevant difference between customer data and customer funds. In this case, the difference which justifies the use of consent is the subjectivity in the value of customer data.

(b) Using Consent to Manage Subjectivity of Data's Value

Although customer data and customer funds are both types of information,[169] the nature of the information is different. For customer funds, the information is the measure of the funds in the unit of account, such as a $100 balance. Because of this measurement, the value of the customer funds is objectively ascertainable and an amount of money in one customer's account with a bank is fungible with the same amount of money in the same type of account of another customer with the same bank. This means that if the customer's funds are lost because of an

165. Foley v. Hill (1848) 9 Eng. Rep. 1002 (HL) 1005-06 (UK).

166. Michael McLeay et al., *Money Creation in the Modern Economy*, 1 BANK OF ENG. Q. BULL. 14 (2014).

167. Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) 5, 21 (Austl).

168. JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 277-78 (2016).

169. *See supra* Part 1(b).

unauthorized transaction on their account then the customer can be compensated by the payment of an amount equal to the value of the lost funds.[170]

However, unlike customer funds, customer data is not fungible.[171] The information derived from one customer's data is not the same as that which can be derived from another's.[172] Although customer data can be measured in bits,[173] this is a measure of the amount of information, not its meaning or, as a result, its value. Although there is no precise way to value data or information,[174] two methods are through the potential gain from its use and the potential loss from its misuse.[175] A customer should value their data because of the gain which its use could provide them (for example by identifying better products or services for them) and because of the loss which it could cause them (for example by enabling unauthorized transactions to be made on their account). However, a different customer may place no value on the first customer's data because its use will not provide them with any gain, and misuse will not cause them any loss. The value of customer data is subjective; it differs depending on the subject's relationship to the information which the data can express. This subjectivity is why a customer cannot be compensated for a loss of their data by sharing another customer's data with them.[176]

170. Other amounts might also be payable such as interest. ARMOUR ET AL., *supra* note 168, at 277.

171. *See* MARTENS, *supra* note 19, at 6. ("Data are not a homogenous product."); *See also* Alec Stapp, *Why Data is Not the New Oil*, TRUTH ON THE MKT. (Oct. 8, 2019), https://truthonthemarket.com/2019/10/08/why-data-is-not-the-new-oil/; VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA (Basic Books 2018).

172. *See* Reimsbach-Kounatze, *supra* note 17.

173. "A *bit* is the smallest unit of information, nothing more than the presence of absence of a signal, a 0 or a 1." FLORIDI, *supra* note 109, at 28.

174. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: THE ESSENTIAL GUIDE TO WORK, LIFE AND LEARNING IN THE AGE OF INSIGHT (2nd ed., 2017); Martens, *supra* note 19, at 4-5; Malgieri & Custers, *supra* note 37, at 294 ("It is sometimes argued that the value of personal data is intangible, risk-dependent, context-dependent and diffuse."); MAYER-SCHÖNBERGER & CUKIER, *supra* note 174, at 104 (noting that determining information's value is complicated by its 'non-rivalrous' nature in that it can be used repeatedly by more than one person, without reducing its functional value to its holder); FLORIDI, *supra* note 109, at 89; Reimsbach-Kounatze, *supra* note 17; ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES AND THEIR CONSEQUENCES 11 (2014) (noting that it is also 'non-excludable' in the sense that it is easily shared, and limiting sharing requires deliberate effort); Joseph E Stiglitz, *The Contributions of the Economics of Information to Twentieth Century Economics*, 115(4) Q.J. ECON. 1441, 1441 (2000); MAYER-SCHÖNBERGER & RAMGE, *supra* note 171, at ____(describing how these factors make it is possible for data to have greater value through secondary and tertiary uses than they might in the use for which the data were originally collected); *See also* MAYER-SCHÖNBERGER & CUKIER, *supra* note 174, at 104.

175. FLORIDI, *supra* note 109, at 89-90 (describing how both price and "the *amount of resources*, such as time, discomfort, or labour, that it would save to its holder" can bring economic value to information).

176. Malgieri & Custers, *supra* note 37, at 298 ("[D]isclosure of personal data may lead to increased risks of future identity theft or fraud, but interpreting such increased risks as actual harm may be too speculative.").

This subjectivity in the value of customer data creates further asymmetry in the relationship between customer and data recipient. Although the customer's data is valuable to them, it is not as valuable to the data recipient. A data recipient is not going to generate as much subjective value from the use of one customer's data as the customer could themselves. Instead, the data recipient's economic gain from customer data is generated by the use of many customers' data at scale and no particular customer's data is likely to be significantly more valuable than any others.[177] This imbalance does not arise with customers' money, where the objective value is the same to the bank and the customer.[178] On a purely economic basis, this means that a data recipient has less economic incentive to take care of a particular customer's data than the customer would themselves. This represents an increased risk for the customer in the data recipient's use of their data.

Requiring customer's consent for the use of their data seeks to manage the risk of loss caused to the customer by the loss or misuse of their data. It is needed because there is no easy way to compensate a customer for the loss of their data and because the data is not as objectively valuable to the data recipient as they are to the customer. Requiring consent seeks to impose control on the data recipient to manage this risk and to make sharing the data safer. Without that control, the customer's position would be similar to its bank being permitted to make withdrawals or transfers from the customer's account without the customer's permission.[179] Accordingly, the reliance on consent should not be considered a flaw in open banking's design but a feature which is intended to improve the risk management in the data sharing. In doing so, it enhances the effectiveness of open banking by enabling the data which is shared to be appropriately used.

3. Summary

The above analysis shows that the requirement for consent is similar in both Australian and UK open banking and that this supports the effectiveness in performing their accountability function. Although there are criticisms of the use of consent in data protection laws, features have been incorporated in open banking in each jurisdiction which are intended to address these issues. It has also shown that there is no similar requirement imposed on a bank to obtain their

177. *See* Buckley at al., *supra* note 5, at 8-9.

178. Even if a bank does not care as much about a particular sum of money as a customer does due to the difference in their respective amounts of money, this does not create a difference in the valuation of the money itself. JOHN ARMOUR ET AL, *supra* note 168 at 278.

179. This would be contrary to the bank's mandate. *See* MARK HAPGOOD, PAGET'S LAW OF BANKING 483 (13th ed. 2007). Arguably, the information on the balance of their account is a better analogy to customer data than the funds actually received by the bank. *Id.* Once the customer's funds are received by the bank, the customer's value is in the 'sum equivalent' recorded in their bank account. *Id.* On this argument, the requirement for consent to use customer data is aligned with the requirement for consent to change the balance of the customer's account. *Id.*

customer's consent for the bank's use of their customer's funds. However, this difference should not be considered a flaw in open banking's design as it is supported by another key difference in the nature of customer data and customer funds, being that the value of customer data is subjective. For this reason, the requirement for consent is needed to balance an asymmetry between the customer and data recipient which would otherwise potentially decrease the fairness of the data exchange. Nevertheless, as with data minimization, the benefits of using consent in the open banking frameworks rely on compliance by the data recipient with the responsibilities which it imposes. Under both frameworks, customers take risk on the performance by the data recipient of its obligations. This risk is even more acute in responsibilities for the integrity of shared data.

V. LEGAL RESPONSIBILITIES FOR INTEGRITY OF SHARED CUSTOMER DATA

The integrity of customer data is fundamental to the effectiveness of open banking. The use of incorrect customer data in open banking, such as in relation to the customer's funds, expenditure, or income, would produce incorrect results potentially both negating the benefits of sharing that data and causing significant loss to the customer or others who rely on the data. This is because for information to have value, it

> *must have some features that are value-adding and value-preserving, such as timeliness, relevance, and updateness. Nobody pays for yesterday's newspaper or the wrong kind of information. Such features go under the general term of information quality.*[180]

The accuracy of shared customer data has been recognised by the CFPB as one of the nine categories of issues addressed in their ANPR.[181] The responsibilities for two key aspects of this, the accuracy and deletion of the shared data, are comparatively analysed below and followed by an evaluation against the responsibilities for the integrity of account information and the bank's obligation to pay under banking law.

1. Comparison of Data Integrity in the Open Banking Frameworks

(a) Accuracy of Data

The responsibilities in Australian open banking for the accuracy of CDR data are found in the requirement in the privacy safeguards to take reasonable steps to ensure that the data are 'accurate, up to date and complete' having regard to the

180. FLORIDI, *supra* note 109, at 90.

181. CONSUMER FIN. PROT. BUREAU, *supra* note 88, at 6.

purpose for which they are held.[182] This obligation applies to both data holders and data recipients each time that they are required or authorised to disclose the CDR data under the *CDR Rules.*[183] What steps are reasonable are determined having regard to the nature of the entity (including its size, resources and complexity of its operations), the sensitivity of the CDR data and adverse consequences to the consumer and the practicability of taking action, including time and cost involved.[184] 'In some circumstances, it will be reasonable for an accredited data recipient to take no steps to ensure the quality of CDR data,' the Office of the Australian Information Commissioner ('OAIC') has noted, '[f]or example, where an accredited data recipient collects CDR data from a data holder known to be reliable.'[185] The result is that data recipients have only a limited legal responsibility for the accuracy of a customer's CDR data, as the obligation arises only if they are required or authorised to share the data and, in any case, it should be reasonable for the data recipient to rely on the correctness of the data. However, if either a data holder or a data recipient becomes aware that data which it has disclosed were incorrect when they disclosed the data, because they were not accurate, up to date and complete at that time, then they must notify the CDR consumer.[186] The CDR consumer can then request that the data be corrected,[187] and that the corrected data be disclosed to the recipient of the earlier disclosure.[188]

GDPR contains the equivalent obligations of accuracy, which is applicable to UK open banking, requiring that personal data are

> *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*[189]

This is combined with a right for a person to rectify 'without undue delay' inaccurate personal data concerning them and to complete such data which are

182. *Competition and Consumer Act of 2010* (Cth.) sub-div 56EN (Austl.).

183. *Id.* at sub-div 56EN(1), (2).

184. Off. of the Austl. Info. Comm'r., *supra* note 122, at ss 11.31, 11.32.

185. *Id*. at s 11.33.

186. *Competition and Consumer Act of 2010* (Cth.) sub-div 56EN (Austl.).

187. *Id.* at sub-div 56EP; The *CDR Rules* require that the data be corrected at no charge. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) rr. 7.14, 7.15 (Austl).

188. *Competition and Consumer Act of 2010* (Cth.) sub-div 56EN(4) (Austl.); *See also Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r. 7.10. (Austl.) (noting that The *CDR Rules* set out notice requirements to the consumer data right (CDR) consumer).

189. Commission Regulations 2016/679, art. 9, 2016 O.J. (L 119) 35 (EU).

incomplete.[190] Unlike the equivalent principles in Australian open banking, this is not specific to the time of disclosure and instead is dependent on the purpose for which the data are being used. For example, if they are being used for a purpose that relies on the data being current, then the data should be kept up to date, particularly if the information could have serious implications for an individual.[191] The reasonable steps are not prescribed as they depend on the purpose for which the data will be used and the significance to an individual of the decisions made using the data.[192] However, it is recognised that it can be impractical to check the accuracy of information which someone else provides and that it is reasonable to assume the accuracy of information provided by a source which is known to be reliable or 'a well-known organisation', unless inaccuracy could have serious consequences or 'if common sense suggests there may be a mistake.'[193]

This comparison shows that the responsibilities for accuracy of shared data are similar in both Australian and UK open banking, and both systems a data recipient should have no responsibility to independently verify the correctness of the customer data received from a bank if they have no reason to suspect it is not correct. Also, under each, the data recipient's responsibility is to take 'reasonable steps' to ensure accuracy, rather than guaranteeing correctness. This is justifiable because, as a matter of practice, the data recipient is not in a position to verify the accuracy of the customer data transferred to it from the customer's bank. Instead, the bank is in the best position, and it owes the obligation to ensure accuracy at the time that it shares the customer data with the data recipient.

(b) Deletion of Redundant Data

The quality of data is impacted by the redundancy of the data as well as its accuracy. This is because '[m]ost data loses some of its utility over time. In such circumstances, continuing to rely on old data doesn't just fail to add value; it actually destroys the value of fresher data.'[194] Accordingly, it is important to analyse how redundant data are removed under Australian and UK open banking.

In Australian open banking, if an accredited person is holding CDR data which they no longer need for the purpose permitted under the *CDR Rules* or the *CCA* (defined as 'redundant data') then they are required to take the steps set out in the

190. *Id*. at art. 16; The term 'inaccurate' is not defined in *GDPR*, but it is taken to mean 'incorrect' or 'misleading' as to any matter or fact. INFO. COMM. OFF., GUIDE TO THE GENERAL DATA PROTECTION REGULATION 35 (Jan. 1, 2021) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

191. *Id*. at 38.

192. *Id*. at 39.

193. *Id.* at 37.

194. *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 174, at 112; *See also* MALGIERI & CUSTERS, *supra* note 37.

CDR Rules to destroy or de-identify that data.[195] Redundant data includes CDR data for which the consent to their use has expired.[196] The *CDR Rules* set out a 'CDR data deletion process' which requires that a person deletes the CDR data and any copies of it, to the extent reasonably practical and direct any other person to whom the person has disclosed the CDR data to also do so.[197] If deletion is not possible, such as when irretrievable destruction from back-up systems is not achievable, then it is sufficient for the data to be put 'beyond use' such that the accredited data recipient is not able to use or disclose the CDR data, cannot give any other entity access to the CDR data, surrounds the CDR data with appropriate technical, physical and organisational security and commits to reasonable steps to 'irretrievably destroy' CDR data when it becomes possible.[198]

GDPR also sets out a right to erasure of personal data, which can also apply to personal data under UK open banking. This requires the data recipient to erase the customer's personal data 'without undue delay' if, most relevantly, the data are 'no longer necessary in relation to the purposes for which they were collected or otherwise processed.'[199] The *GDPR* process also applies to all backup systems which record those data. Similarly, where deletion in the backup systems takes time (because, for example, it needs to be overwritten by new data) the data must be put 'beyond use' and not used for any other purpose.[200] Because *GDPR* is limited to personal data, the right of erasure does not apply to business account data under UK open banking. However, the requirements of *PSR* still apply and as analysed above, the data are not able to be used for any other purpose,[201] even though there is no right to require deletion.

Other than the recurring issue of the limitation of the application of *GDPR* to personal data, the requirements for deletion of redundant data are broadly comparable under open banking in Australia and the UK. Where the treatment of redundant data differs is in the ability to de-identify and reuse redundant data. The *CDR Rules* set out a 'CDR data de-identification process' which enables a de-identification technique to be used on redundant data instead of deletion.[202] This can be used by a data recipient if it ensures that no person is identifiable, or

195. *Competition and Consumer Act of 2010* (Cth.) sub-div 56EO (Austl.).

196. Off. of the Austl. Info. Comm'r., *supra* note 122, at para 12.77.

197. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) r 1.18 (Austl.); *See* Off. of the Austl. Info. Comm'r., *supra* note 122, at para 12.106 (discussing that the reasonably practical inquiry includes taking into account the amount of CDR data, the nature of the accredited data recipient and its information handling practices, and the possible adverse consequences for a consumer and the practicability, including the time and cost involved).

198. Off. of the Austl. Info. Comm'r., *supra* note 122, at para 12.108.

199. Commission Regulation 2016/679 of Apr. 27, 2016, art. 9, 2016 O.J. (L 119) 17 (EU).

200. INFO. COMM. OFF., *supra* note 190, at 118.

201. *See supra* Part IV, 1(a).

202. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) r 1.18 (Austl.).

reasonably identifiable, from the data after de-identification taking into account any other information held by any other person.[203] Additionally, the CDR consumer needs to have consented to de-identification, the accredited person must have given the CDR consumer a statement of further information on de-identification, the CDR consumer must not have elected for the CDR data to be deleted and the accredited person must think it appropriate in the circumstances to de-identify rather than delete the CDR Data.[204] Redundant data which has been de-identified in accordance with this process may be disclosed to any person, including by sale.[205]

Whilst a similar concept exists under *GDPR* in that it ceases to apply to personal data which have been rendered anonymous in such a way that the data subject is no longer identifiable,[206] the *PSR* does not permit the information shared to be anonymized for use for another purpose.[207] Also, although *GDPR* sets out conditions for the processing of personal data for purposes other than for which they have been collected,[208] such as where the customer has given their consent or where the processing is compatible with the initial purpose, these are not applicable to data shared under UK open banking.[209] Accordingly, the re-use of redundant data is not facilitated under the UK framework, even if anonymized.

The ability to de-identify and re-use shared data represents a potentially significant difference between Australian and UK open banking. The ability to re-

203. *Id.*

204. *Id.* at rr 4.11, 4.15 – 4.17, 7.12.

205. *Id*. r 7.5(1).

206. INFO. COMM'RS. OFF., ANONYMISATION, *Anonymisation: Managing Data Protection Risk Code of Practice* (Nov. 2012),https://ico.org.uk/media/1061/anonymisation-code.pdf.

207. UK Finance notes that although there should be "little customer detriment" in using anonymized open banking data for the purpose of assessing the account information service and making improvements, this would "on a strict interpretation of the PSRs" not be permissible. UK FINANCE, *supra* note 140, at 7; The European Banking Federation has noted that this would "prevent a range of legitimate and important data processing activities." EUR. BANKING FED'N, *EBF Response to the European Data Protection Board's Consultation on the Guidelines of 6/2020 on the Interplay of the Second Payment Services Directive and the GDPR,* EUR. BANKING FED'N at 5 (Sept. 16, 2020), https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/ebf_042474_-_european_banking_federation_response_edpb_guidelines_psd2-gdpr_.pdf.

208. Commission Regulations 2016/679 of Apr. 27, 2016, art. 6, 2016 O.J. (L 119) 36-7 (EU).

209. The European Data Protection Board (EDPB) has stated that, based on the particular wording of *PSD2*, further use with consent, but not compatibility with initial purpose, is applicable to data received under *PSD2*. EUR. DATA PROT. BD., *supra* note 96, at ¶ 22; However, the wording relied on by the European Data Protection Board, "in accordance with data protection rules" from the EU Directive 2015/2366 is not included in the Payment Services Regulations. *See* Directive 2015/2366/EU of the European Parliament and of the Council of Nov. 25, 2015, Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, O.J. (L 337) 35 at art. 67(2)(f); The Payment Services Regulations 2017, SI 2017/752, art. 70, ¶ (3)(f) (UK); Accordingly, the information received under the UK framework cannot be used for any other purpose. *See* UK FINANCE, *supra* note 140, at 7; *See also* FIN. CONDUCT AUTH., *supra* note 85, at 222.

use information increases its value and 'data's full value is much greater than the value from its first use.'[210] One way in which this increase in value occurs is through combining the data with other data sets, to produce insights not otherwise available.[211] From an economic perspective, the option to re-use customer data is accretive in its value, and 'the data's worth is the sum of these choices.'[212] Accordingly, the inclusion of the ability to re-use customer data increases the potential benefits of Australian open banking.[213]

However, the conditions for exercising the right to de-identify and re-use data under Australian open banking are not easily met. The requirement that is the most difficult to meet is that 'no person would any longer be identifiable, or reasonably identifiable, from … other information that would be held, following the completion of the de-identification process, by *any person*.'[214] This implies no risk of re-identification assuming an 'open release environment' even if open release is not intended.[215] It is doubtful that this standard can be currently met as a technological matter, particularly as OAIC and Data61 (part of the Australian government's national science agency) have previously stated that 'after de-identification, risk is still generally not zero.'[216] As a result, 'there is significant complexity and risk involved with attempting to de-identify unit record data derived from CDR data to the "required extent" as defined in the CDR Rules.'[217] Accordingly, it should not be expected that any significant benefits derived from de-identification under Australian open banking will be available unless further clarity is provided of what standard of de-identification is needed,[218] and the technical possibility of de-identification is not a meaningful difference between the frameworks. Nevertheless, it is submitted that the standard for de-identification to re-use customer data in the open banking frameworks should not be more restrictive than under data protection laws. Otherwise, this could result in regulatory arbitrage with

210. *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 174, at 104 (discussing how "valuable data's refuse can be").

211. *Id.* at 111 (highlighting how many big companies, like Google and Microsoft, reuse past data and combine it with other data sets, showing that "[t]he reuse of data can sometimes take a clever, hidden form").

212. *Id.* at 104.

213. Although this is not likely to directly benefit the relevant customer. *See id.* at 105.

214. *Competition and Consumer (Consumer Data Right) Rules*, *2020* (Cth) s 1.17 (Austl) (emphasis added).

215. Off. of the Austl. Info. Comm'r., *supra* note 122, at para 12.96.

216. OFF. OF THE AUSTL. INFO. COMM'R., *De-Identification Decision-Making Framework*, at ix (Sept. 18, 2017); The complexity of this issue is increased in that the *CDR Rules* require that a data-recipient has regard to this framework in making its determination that there is no risk of re-identification.*See Competition and Consumer(Consumer Data Right) Rules 2020* (Cth) sub-div 1.17 (Austl).

217. In an earlier (October 2019) draft of these guidelines, the Office of the Australian Information Commissioner was even more negative. *See* Off. of the Austl. Info. Comm'r., *supra* note 122, at para 12.99.

218. AUSTRALIAN COMPETITION AND CONSUMER COMMISSION *Explanatory Statement, Competition and Consumer (Consumer Data Right) Rules* 2020 (Cth) 15 (Austl.). The Australian Competition and Consumer Commission has further recommended that a data standard be produced for de-identification.

data recipients preferring to collect data outside the open banking frameworks so that the data can be more easily used.[219] This would deprive customers of the other benefits and protections of the open banking frameworks analysed in this and the previous chapter.

2. Evaluation Against Customer Rights in Bank Accounts

(a) Comparison with Integrity of Account Information

The promise of 'storage' of value is at the foundation of banks' relationships with their customers and, as the customer's funds are represented by the credit balance owing by the bank on their customer accounts, this is provided through the integrity of the records of those accounts.[220] The account which represents that record is the core of the banker – customer relationship.[221] Although the method used to share this information with customers has changed over time, from passbook,[222] to bank statements, to electronic access to bank accounts, customers have been granted an ability to rely on the correctness of the bank's records in good faith, even if the account had been over-credited by mistake.[223] Further, a bank customer has no implied duty to check bank statements relating to the customer's account, or notify the bank of any errors or unauthorized transactions.[224] Unauthorized changes to the customer's account are dealt with as a matter of the core functions and duties of a bank, and not as a failure of operational requirements.[225] From this

219. For example, data recipients might revert to screen scraping where that is permitted. *See Competition and Consumer Act of 2010* (Cth.) (Austl.). Also, it provides an advantage to ADIs who can, for particular customer data which they receive under the Australian framework, be treated as being subject to the *Privacy Act* rather than the *CCA*. *See Competition and Consumer Act of 2010* (Cth.) (Austl.); *See supra* note 118 and accompanying text.

220. This can be described as "custodial storage" and "most custodial storage today takes place on the electronic accounting systems" of banks. AWREY & ZWIETEN, *supra* note 29, at 782.

221. *See* Hart v. Sangster (1957) 2 Eng. Rep. Ch 337 (UK); *See* Ladbroke & Co v. Todd (1957) Eng. Rep. 1134 (UK).

222. The passbook was a copy of the customer's account in the ledger of the bank: FRANCIS ALFRED ALISON RUSSELL, THE LAW RELATING TO BANKER AND CUSTOMER IN AUSTRALIA 81 (1935).

223. *See* G. A. WEAVER & C. R. CRAIGIE, THE LAW RELATING TO BANKER AND CUSTOMER IN AUSTRALIA 224 (The L. Book Co. Ltd.,1975); W.S. WEERASOORIA, BANKING LAW AND THE FINANCIAL SYSTEM IN AUSTRALIA 410 (2nd ed., 1988).

224. *See* Tai Hing Cotton Mill Ltd. v. Liu Chong Hing Bank Ltd. (1986) AC 80 (UK). This allows the customer to honestly take the benefit of an error in their account (such as an erroneous credit entry) if the customer alters their position in reliance on the entry in good faith; *See* Holland v. Manchester and Liverpool District Banking Co Ltd (1909) 25 T.L.R. 386; Lloyds Bank Ltd. v. Brooks (1950) 6 LDAB 161 (UK); However, it does not permit a customer to knowingly take advantage of an error. Foley v. Hill (1848) 2 HL Cas. 28, 36 (UK).

225. For example, the case of British and North European Bank v. Zalzstein concerned the unauthorized amendment of the bank's customer's passbook to change the amount owed by the bank to the customer. Although this was a case of unauthorized alteration of information records, it was dealt with on the basis of the rights between bank and customer to recover funds. *See* British and North European Bank Ltd. v. Zalzstein (1927) 2 KB 92 (UK).

it can be seen that the bank's responsibility to ensure the integrity of the information constituting the customer's account is clear and direct.

This is not the same under open banking. As Part 5.1 shows, the data recipient has little real responsibility to maintain accuracy of the shared data. It could be argued that this represents a weakness in open banking's design due to the importance of accuracy to the value of that data. It would follow from this argument that the data recipient should be responsible to the customer for the quality of the customer's account information in the same unqualified way that a bank is responsible for the integrity of the customer's account. However, this argument does not consider the difference in the legal relationship which each of the bank and the data recipient have with the customer account information. For the bank, the information measures and defines its obligation to repay the amount received on behalf of the customer. Its content, and as a result its accuracy, is fundamental to the bank's legal obligations. For the data recipient, the information is something valuable which has been shared with it by the customer to be used for a particular purpose. The information's content is *why* it is valuable, but the data recipient's obligations are *not defined by* that content. The responsibilities of the data recipient to the customer are unchanged by the meaning of the information shared with it. In concept, the difference in obligation is similar to that which a bank would owe under a debenture which it issued to a customer, and the obligation which the bank would owe to a customer in respect of a debenture which it held in safe custody. Whilst the bank's obligations under its debenture are clear and direct, the bank does not have unqualified responsibility for any loss of value of what it holds in safe custody, as its liability is based in either negligence or conversion.[226] Consequently, it does not follow that the same unqualified obligation owed by the bank needs to be imposed on the data recipient. Further, given that the data recipient would find it nearly impossible to discharge that obligation, it would not enhance the effectiveness of the frameworks to do so. For these reasons, the absence of an equivalent clear and direct obligation to ensure the information's integrity should not be regarded as a deficiency in the frameworks' design.

(b) Comparison with a Bank's Obligation to Repay

The most fundamental of a bank's responsibilities to its customer is to repay the amount of the customer's funds. The contract between bank and customer includes 'the promise to repay [the funds] … at the branch of the bank where the account is kept' and 'a promise to repay any part of the amount due against the written order of the customer.'[227] Although repayment by the bank of the amount

226. *See* HAPGOOD, *supra* note 179, at 483; *See also* WEERASOORIA, *supra* note 223, ch. 27.

227. Joachimson v. Swiss Bank Corporation (1921) 3 KB 110, 127 (UK).

demanded by the customer is made from the bank's own funds rather than the actual funds received for the customer, its effect is to reduce the bank's ability to use funds of an amount equal to those originally received. Repayment discharges the bank's responsibilities to the customer for those funds and discharges the bank's obligation to repay them.

Transfer of the data back to the customer by the data recipient does not discharge the data recipient's obligations in the same way. Data is non-rivalrous, meaning that both the bank and the customer can use and share the customer data at the same time.[228] Accordingly, the transfer of the data back to the customer does not prevent the data recipient's further use of the data. Instead, to prevent the data recipient's use, the data recipient must delete all its copies of the data.

In one sense, the position of the customer in relation to the repayment of their funds is similar to the customer's position in relation to the deletion of their data. In both circumstances, the customer is exposed to risk of non-performance by the bank or data recipient. However, the risk taken by a customer with respect to their funds lasts only until they are repaid.[229] This payment settles the bank's obligations because the client accepts the funds as a 'settlement asset,'[230] and the repayment can be verified by the customer by their receipt of the amount of their funds. There is no equivalent in open banking as there is no settlement asset which the customer can accept in discharge of the data recipient's obligations. Although the risk taken by a customer with respect to their data also should only last until they can verify that it has been deleted, the customer has no way of making that verification unless the data recipient's systems are audited, and neither framework requires this to occur. Accordingly, the customer takes ongoing risk that the data recipient has in fact performed its obligations and is not continuing to use, replicate and share the customer's data without the customer's knowledge. Non-compliance by the data recipient could result in the customer's banking information being improperly used on a vast scale and significantly impair the effectiveness of open banking. This is a key difference between data sharing under open banking and funds transfers in banking. Of itself, it is not a flaw in the design of open banking, as it is a direct consequence of the difference between customer data and customer funds. However, the absence of the verification mechanism required to manage the consequence of that difference is a risk that should be managed.

228. MAYER-SCHÖNBERGER, *supra* note 174, at 104.

229. Assuming that no insolvency-related 'clawback' provisions (such as those related to unfair preferences) subsequently applies.

230. A settlement asset is an asset which a creditor can accept in final settlement of the obligation owed to it. *See* MARK MANNING ET AL., THE ECONOMICS OF LARGE-VALUE PAYMENTS AND SETTLEMENT: THEORY AND POLICY ISSUES FOR CENTRAL BANKS 1 (2009).

3. Summary

The above analysis shows that that the responsibilities of data recipients for the integrity of shared data are similar in open banking in Australia and the UK. It differs from the unqualified obligations of a bank for the correctness of the records of the customer's account. This difference is justifiable given the different relationship between the information and the customer. Although the information held by the data recipient is valuable to the customer, it does not define the responsibilities of the data recipient in the same way that the account balance does for a bank's responsibilities.

The analysis shows that the requirements for the deletion of customer data when they are no longer needed are not significantly different between the jurisdictions. The analysis also shows that the requirement to delete customer data is conceptually similar to the bank's obligation to repay customer funds. However, the unavailability of a settlement asset and the absence of an ability for the customer to verify that their data has been deleted means that the customer continues to be exposed to the risk of the data recipient's non-performance for as long as the data are valuable. As with the performance of data minimization and data use responsibilities, this represents a potential risk to be addressed in the design of open banking. This risk, which relates to the trust placed in data recipients' performance of their obligations is managed in open banking through the authorizations required to receive customer data.

VI. Legal Responsibilities in Authorisation to receive Customer Data

Customer trust is a vital element in making open banking frameworks work effectively.[231] Trust 'gives people confidence to place their faith in strangers and systems.'[232] Trust is fundamental to the effectiveness of open banking because of the reliance which is placed on the performance by the data recipient of its responsibilities to ensure the safe storage and appropriate use of shared data. Both frameworks impose requirements for authorization to receive shared data to help establish that trust.[233] Those requirements are designed to meet two key elements needed for this purpose, namely that 'data is handled safely'[234] and 'there's redress

231. Consumer trust is crucial for CDR's success." DATA STANDARDS BODY & CONSUMER POL'Y RSCH. CTR., STEPPING TOWARDS TRUST, at 3 (Report, Aug. 2020); "The success of Open Banking will depend on whether it can engage consumers and earn their trust." FAITH REYNOLDS ET AL., CONSUMER PRIORITIES FOR OPEN BANKING, at 41 (Report, June 2019).

232. PHILIPPA RYAN, TRUST AND DISTRUST IN DIGITAL ECONOMIES 13 (2019).

233. "Consumers will only be able to use the right to direct the transfer of their data to trusted third parties. All data recipients who receive consumer specific data must be accredited." COMMONWEALTH TREASURY, *supra* note 44, at 7.

234. DATA STANDARDS BODY & CONSUMER POL'Y RSCH. CTR., *supra* note 231, at 21; "Data protection is a key factor in building trust between business and customers." RYAN, *supra* note 232, at 85; Research has found that due

when things go wrong.'[235] The responsibilities for these two key foundations of this trust, information security and customer compensation, are comparatively analysed below, followed by an evaluation against the management of information security and deposit protection in banking payment systems.

1. Comparison of Responsibilities for Information Security and Compensation

(a) Information Security

Under Australian open banking, in order to be accredited to receive customer data, a data recipient must take prescribed steps to protect CDR data from misuse, interference and loss, unauthorized access, modification and disclosure.[236] The steps are operational in nature: to define and implement security governance, define the boundaries of the CDR data environment, have and maintain an information security capability, implement a formal controls assessment program and have plans to manage and report security incidents.[237] The *CDR Rules* also require there to be Australian Standards about the security of CDR data,[238] and the Australian Standards contain specific security profiles which are required to be met.[239]

to the 'perceived and actual risk of privacy loss and identity theft', trust in the government and in the participants in the framework has been found to 'play a vital role' in the decision of customers to use the Australian framework. Nicholas Biddle & Dinith Marasinghe, *Risky Data: The Combined Effect of Framing, Trust and Risk Preferences in the Intended Participation in the Consumer Data Right* (Tax and Transfer Pol'y Inst., Working Paper No. 9/2019, Oct., 2019).

235. FAITH REYNOLDS ET AL., *supra* note 231, at 41; "With personal data being the lifeblood of the digital economy, its free flow is built on consent, and trust is crucial." INT'L TELECOMM. UNION, POWERING THE DIGITAL ECONOMY: REGULATORY APPROACHES TO SECURING CONSUMER PRIVACY, TRUST AND SECURITY, 36 (Piers Letcher, ed., 2018).

236. *Competition and Consumer Act of 2010* (Cth.) sub-div 56EO (Austl.); This obligation is repeated in the CDR Rules. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) r 5.12(1)(a) (Austl.); Whilst these terms are not defined, the OAIC gives them a comprehensive meaning, including the use of CDR data for a purpose not permitted by the CDR, attacks on CDR data that interferes with them but does not modify their content, the accidental or inadvertent loss of the CDR data where they are no longer accessible or useable for their purpose, access by someone who is not permitted to do so, the alteration of CDR data in a way which is not permitted, and where an accredited data recipient makes CDR data accessible to others outside the entity. OFF. OF THE AUSTL. INFO. COMM'R., *supra* note 122, at s 12.17.

237. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) r 7.11, sch 2 (Austl.); Similarly, the "minimum information security controls" needed for the required information security capability are procedural - the data recipient must have processes in place to limit the risk of inappropriate or unauthorized access, take steps to secure their network and systems and to limit prevent and remove malware, implement formal programs on vulnerability management and information security training and 'securely manage' their information assets. *Id*.

238. *Id*. at r 8.11.

239. CONSUMER DATA STANDARDS, CONSUMER DATA STANDARDS v 1.16.0 https://consumerdatastandards.gov.au/consumer-data-standards/current-reference (last visited Feb. 2, 2022).

The information security requirements under UK open banking are similar. The *CMA Order* requires that the UK Standards include security standards.[240] Accordingly, specific security profiles are included,[241] and further detailed security guidelines have been provided by the OBIE.[242] The *PSR* requires that data recipients must have a security policy and procedure for monitoring, handling and following up security incidents, and a statement of the applicant's security policy.[243] The *PSR* also requires an AISP to establish a risk management framework for operational and security risks.[244] In line with these,[245] the FCA has directed that AISPs comply with guidelines on security measures issued by the European Banking Authority in respect of *PSD2*.[246] An AISP is also required to notify the FCA of any major security incident, and its customers if it has, or may have, an impact on their financial interests.[247] In addition to the *PSR* requirements, *GDPR* has its own security obligations, requiring that open banking data which are personal data, are processed in a manner which ensures 'appropriate security',[248] including through 'protection against unauthorized or unlawful processing and against accidental loss, destruction or damage' by means of appropriate technical and organisational measures.[249] No specific security measures are required by *GDPR* as the requirements depend on the particular context.[250]

240. CMA ORDER, *supra* note 74, at ¶ 10.2.3. (UK).

241. SECURITY PROFILES*, Financial Grade API (FAPI) Profile,* OPEN BANKING, https://standards.openbanking.org.uk/security-profiles/ (last visited Feb. 7, 2022).

242. OPEN BANKING IMPLEMENTATION ENTITY, OPEN BANKING GUIDELINES FOR READ/WRITE PARTICIPANTS, OPEN BANKING (May 2018), https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf.

243. Payment Services Regulations, *supra* note 75, regs. 17, sch. 2. Registration to provide account information services under the *PSR* requires a statement of the applicant's security policy, including a detailed risk assessment in relation to the payment services to be provided (such as risks of fraud and illegal use of sensitive and personal data), and a description of the applicant's security control and mitigation measures.

244. *Id*. at reg. 98(1).

245. *See* FIN. CONDUCT AUTH., FCA HANDBOOK (2013), https://www.handbook.fca.org.uk/instrument/2013/FCA_2013_8_PRA_2013_3.pdf; *See also* FIN. CONDUCT AUTH., *supra* note 85, ¶ 18.3.

246. These cover operational matters such as governance, risk assessment, protection, detection, business continuity, testing, situational awareness and continuous learning and customer relationship management. EUR. BANKING AUTH., *Guidelines on the Security Measures for Operational and Security Risks of Payment Services under Directive (EU) 2015/2366 (PSD2)* (Final Report No. EBA/GL/2017/17, Dec. 12, 2017).

247. Payment Services Regulations, *supra* note 75, reg. 98.

248. Commission Regulation 2016/679 of Apr. 27, 2016, art. 5(1)(f), 2016 O.J. (L 119) 17 (EU).

249. *Id*. at art. 32(1).

250. INFO. COMM'R. OFF., *supra* note 190, at 271; The European Data Protection Board has noted the severity of the risks involved in financial personal data and concluded that, as a result, 'the security measures must be accordingly high' EUR. DATA PROT. BD., *supra* note 96, at 21.

Without going into the technical detail of the requirements,[251] each jurisdiction requires data recipients to adhere to a security profile based on similar technical foundations.[252] Also, the breadth of coverage under each framework is similar in that each addresses the broad information security concepts of confidentiality (preventing unauthorized disclosure), integrity (preventing unauthorized modification) and availability (ensuring that information is available to be processed and transmitted).[253]

It is noteworthy that neither jurisdiction imposes significant direct obligations on data recipients to ensure the security of data even though, in the case of Australian open banking, the purpose of the information security privacy safeguard is 'to ensure that CDR data is protected from misuse, interference and loss as well as from unauthorized access, modification or disclosure,'[254] and in the case of the UK framework, the OBIE is to 'ensure that customers are fully protected against privacy and security risks.'[255] Instead, as noted above, the obligations are operational and procedural, and framed as being to take 'reasonable steps.' The UK framework does contain one clear security-related obligation on AISPs, which is to ensure that the customer's personalised security credentials are 'not accessible to other parties.'[256] However, this is not a point of material difference between the jurisdictions as the Australian open banking does not allow access to account data using the customer's security credentials so these should not be held by the data recipient.[257] This absence of direct security obligations is evaluated further in Part 6.2 below with respect to the equivalent obligations in banking regulation.

(b) Customer Compensation

Under Australian open banking, CDR consumers have a statutory right to take direct action against an accredited person for the damages caused by the entity's non-compliance.[258] Similarly, under UK open banking, there is a direct right of action contained in the *PSR* for 'private persons' that suffer loss as a result of a contravention of the *PSR*.[259] Neither framework requires a data recipient to hold a

251. A technical analysis of the security requirements is beyond the scope of this article.

252. *See* OPEN BANKING *supra* note 241.

253. JASON ANDRESS, FOUNDATIONS OF INFORMATION SECURITY: A STRAIGHTFORWARD INTRODUCTION 3 (2019).

254. THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA, *Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018* (Cth) ¶¶ 1.15, 1.372 (Austl.).

255. COMPETITION AND MARKET AUTHORITY, *Retail Banking Market Investigation Order 2017, Explanatory Note* at 40 (UK).

256. Payment Services Regulations, *supra* note 75, reg. 70(3)(b).

257. See *supra* note 18 (Working similarly to UK open banking, Australian open banking relies on the use of APIs.).

258. *Competition and Consumer Act*, *supra* note 6, s 82(1)(d).

259. Payment Services Regulations, *supra* note 75, reg. 148.

minimum amount of capital to ensure that it is able to meet these liabilities.[260] Instead, under each framework, in order to be authorised, a data recipient must have adequate insurance, or a comparable guarantee.[261] In Australian open banking, this is required 'in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations' under the *CCA*, any regulations made under it, or the *CDR Rules*, to the extent they are relevant to the management of CDR data.[262] However, it is not required for accredited persons that are Authorised Deposit-taking Institutions.[263] In UK open banking, it is required to cover 'the applicant's potential liability to account servicing payment service providers and payment service users resulting from unauthorized or fraudulent access to, or use of, payment account information, up to such amount as the FCA may direct.'[264]

The purpose is subtly different under each framework. In the UK, it has the purpose of 'strengthening the liability regime governing the interactions between the different actors involved in electronic payment transactions.'[265] Capital is not required under UK open banking because data recipients do not hold customer's funds.[266] A slightly different justification is given under Australian open banking, namely to 'reduce the risk of CDR consumers not being properly compensated due to an accredited person's lack of financial resources'.[267] For this reason, data recipients that are ADIs are exempt from the requirement to obtain insurance,[268] as their prudential regulation and capital requirements should adequately ensure sufficient financial resources to compensate CDR consumers. Although under each

260. *Id.* reg. 6(3).The UK framework does require minimum capital be held by providers of other payment services.

261. *Competition and Consumer Rules 2020* (Cth) r 5.12(2)(b)(Austl); Payment Services Regulations , *supra* note 75, reg. 18(4).

262. *See supra* note 261.

263. *Id*. sch 3 r 7.4(2).

264. Payment Services Regulations, *supra* note 261; For this purpose, the FCA has directed that the amount be that which is determined in accordance with guidelines issued by the European Banking Authority in respect of

PSD2: FIN. CONDUCT AUTH., *supra* note 85, at ¶ 3.59; The guidelines are issued under Article 5(4) of *PSD2*: The guidelines are issued under Article 5(4) of *PSD2*: The guidelines are issued under Article 5(4) of *PSD2*: EUROPEAN BANKING AUTHORITY, *Guidelines on the Criteria on How to Stipulate the Minimum Monetary Amount of the Professional Indemnity Insurance or Other Comparable Guarantee under Article 5(4) of Directive (EU) 2015/2366* (Final Report No. EBA/GL/2017/08, July 7, 2017); The effect of this requirement under *PSD2* has been described as being to "promote consumer confidence" and that it "allows consumers to focus on things of value instead of worrying about the possibility of monetary loss". Adebola Adeyemi, *A New Phase of Payments in Europe: the Impact of PSD2 on the Payments Industry*, 25 COMPUT. & TELECOMM. L.R. 47 (2019).

265. EUR. BANKING AUTH., *EBA Publishes Final Guidelines on Professional Indemnity Insurance* (Press Release, Jul. 7, 2017).

266. Payment Services Regulations, *supra* note 261, sch. 3 pt. 1(2); *See also PSD2*, *supra* note 7, recital 35.

267. AUSTL. COMPETITION & CONSUMER COMM., ACCREDITATION GUIDELINES 14 (Dec. 9, 2020).

268. CDR RULES, *supra* note 6, at sch. 3.

framework insurance is required to take the place of the data recipient's capital in covering liabilities, in Australia it does so on the assumption that the data recipient won't hold enough capital to cover its liabilities unless it is a bank, whilst in the UK it does so on the assumption that the data recipient should not be required to hold enough capital to cover its liabilities unless it also holds customers' money. Each of these assumptions is flawed in context of large technology companies becoming data recipients (who would be required to obtain insurance despite having sufficient economic capacity to meet any claims) and the increasing recognition of the value of customer information (which would mean that both money and information are valuable to the customer). However, the impact of these flaws is small compared to the issues which arise in relying on indemnity insurance to ensure the data recipient's creditworthiness and performance. This analysis is continued in Part 6.2(b) below.

Another difference is in relation to the scope of the insurance. Under UK open banking it is to compensate for claims made by both banks and customers but only in respect of unauthorized or fraudulent access or use of customer data. Under Australian open banking, the insurance is to compensate for claims by customers only, but it is not limited to particular types of claims. In different ways, the scope of each is more limited than the other, either with respect to the object of the covered liability or the nature of the liability covered. The UK limitation should not be practically meaningful, as it is difficult to see the sources of the data recipient's liability relating to the shared data beyond those which relate to the unauthorized or fraudulent access or use of those data. There could be liability for the account information services provided by the AISP if they are performed negligently. Theoretically these might not be covered by the required insurance, but neither would they be covered by insurance under the Australian framework as the insurance is not required to cover the provision of the goods or services requested by the customer.[269] In contrast, the limitation on insurance in Australian open banking is more significant. The absence of a requirement for insurance to cover liabilities owed to persons other than customers is anomalous as the data recipient has potential liabilities to banks as well under Australian open banking.[270] Arguably, it reflects the compensation provisions to protect retail clients of holders of an Australian Financial Services License under the Australian *Corporations Act 2000* (Cth).[271] However, that regime does not contemplate a network of regulated entities sharing responsibilities.

269. These are not obligations owed under the *CDR Rules.*

270. The *CCA* creates a separate contract between a data holder and each accredited person. CCA, *supra* note 6, at ss 56FD(1)(a)-(b).

271. Holders of an Australian Financial License must have compensation arrangements for retail clients to cover losses suffered as a result of breaches by the licensee: *Corporations Act 2001* (Cth) s 912(d) (Austl.).

2. Evaluation Against Information Security and Deposit Protection in Banks

(a) Management of Information Security Risk in Banks

Information security has always been critical to banking and payments.[272] Information security issues can compromise the core functions of banking, affect the trust in which the system is held,[273] and the confidence in banking as a whole.[274] In this context, the use of digital records has caused information integrity to be a central challenge in banking and payments.[275]

The regulatory framework applicable to banks seeks to manage this risk by imposing information security obligations, such as the requirements of the Australian Prudential Regulation Authority,[276] and the Prudential Regulation Authority of the UK.[277] These treat information security as part of operational risk management.[278] As a result, it is regulated through procedural requirements, governance arrangements and general duties which are broadly, and sometimes obscurely, described.[279] This principles-based approach is intended to avoid both inflexibility in the face of changing technology, and overregulation.[280]

The security requirements of Australian and UK open banking take a comparable approach, adopting an operational perspective, rather than imposing direct and positive obligations. This similarity is not surprising given the foundational role that banks perform as data holders in open banking and the desirability of not transferring customer data from a high information security environment to one

272. "Data should be protected from loss and leakage, unauthorised access, and other processing risks, such as negligence, fraud, poor administration, and inadequate recordkeeping": Comm. on Payment & Settlement Sys. & Int' Org. of Sec. Comm'ns, *Principles for Financial Markets Infrastructures*, at ¶ 3.17.12 (Bank for Int'l Settlements Report, Apr., 2012).

273. *Gottfried Leibbrandt on Cyber Security and Innovation*, SWIFT (May 24, 2016), https://www.swift.com/news-events/press-releases/gottfried-leibbrandt-cyber-security-and-innovation.

274. *See* RESERVE BANK OF AUSTRALIA, FINANCIAL STABILITY REVIEW (Oct. 2018).

275. "Increased use of technology and digital records in banking, such as the introduction of open banking over the coming year, could raise additional cyber risks." *Id.* at 55; *See also* Bank of Eng., *Future of Finance. What it means for the UK Financial System,* at 3, 14 (June 2019); "[A]n attack that had implications for the integrity of banks' record of their assets and liabilities could impede their ability to disburse funds to customers or collect on monies due. In the extreme it could raise questions about the institution's solvency status. This could force directors to withdraw the bank from trading while investors may pull back on capital market funding." *Id.* at 57.

276. APRA Prudential Standard CPS 234, *Information Securit*y (July, 2019) (Aus.).

277. PRUDENTIAL REGUL. AUTH., CBEST THREAT INTELLIGENCE-LED ASSESSMENTS (2021).

278. Comm. on Payment & Settlement Sys. & Int' Org. of Sec. Comm'ns, *supra* note 272, at ¶ 2.9; *See also* Anton Didenko, *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond*, 25 UNIF. L.R. 125 (2020).

279. "For example, PSD2 refers to 'operational and security risks' throughout Article 95 but the difference between the two risk types is vague at best." Didenko, *supra* note 278.

280. *Id.*; *See also* Eur. Banking Auth., *supra* note 246, at 27.

with lower information security. However, it does raise the question as to whether positive and unqualified obligations to keep customer data secure should be imposed for the frameworks.[281] By comparison, a bank's obligation to repay its customer's funds is a direct and positive obligation, not qualified by any theft or cyber-security attack to which the bank has been subject.[282] Taking a similar approach in open banking would impose an unconditional obligation on data recipients to ensure that customer data are 'not accessible' to other persons. However, for the reasons discussed in Part 5 above, a bank's responsibility for the integrity of the balance of the customer's account is not the correct benchmark. Instead, the correct benchmark is the bank's responsibility for the safe custody of the customer's valuables. A bank is not liable for the theft of such assets if there is no negligence or conversion by the bank or its employees.[283] Accordingly, the absence of an unqualified and direct obligation to keep the customer's data secure should not be considered a flaw in open banking's design.

(b) Role of Deposit Protection for Banks

Bank regulation not only ensures that bank's promises *can* be met but also provide confidence to depositors that they *will* be met. Without this, if there is any disruption to a bank, depositors may seek to withdraw funds at the earliest opportunity, threatening the solvency of the bank as illiquid assets are sold at a loss to meet depositors' claims.[284] This 'confidence trick' on which banking is based works so long as depositors believe (a) the bank's investments are safe and will yield the returns that they promise, and (b) other depositors will not withdraw more than their customary amounts.[285]

Deposit protection is an important support for this confidence. It provides depositors with assurance from a third party that their claims will be met if the bank defaults.[286] 'This third party thus effectively steps into the shoes of the bank, honoring the bank's commitment to provide depositors with both storage and liquidity during periods of institutional stress.'[287]

281. The obligations to not disclose data do not cover the prevention of unauthorized access. *See* OFF. OF THE AUSTL. INFO. COMM., *supra* note 122, at ¶ B.114.

282. *See supra* Part V 2(a).

283. *See supra* note 226 and accompanying text.

284. "[E]veryone rushes in to withdraw their deposits before the bank gives out all of its assets. The bank must liquidate all its assets, even if not all depositors withdraw, because liquidated assets are sold at a loss." Douglas W Diamond & Philip H Dybvig, *Bank Runs, Deposit Insurance, and Liquidity*, 24 FED. RSRV. BANK OF MINN. Q.R. 15 (2000); *See also* ARMOUR ET AL., *supra* note 168, at 48.

285. ARMOUR ET AL., *supra* note 168, at 278.

286. *Id*. at 332.

287. Awrey & Zwieten, *supra* note 29, 795.

The insurance required to be held by data recipients is intended to perform a similar function in each open banking framework – to guarantee the creditworthiness of the data recipient sufficiently for claims against it to be met. However, its ability to perform this function is impaired when compared with deposit protection. This is because the insurance contemplated is professional indemnity insurance,[288] which does not entitle the customer to claim directly against the insurer.[289] Instead, the data recipient is required to make a claim and the amount received increases the assets which it has available to compensate others.[290] However, the data recipient will not be able to do so if it is in breach of its contractual policy obligations, the claim falls under a policy exclusion, the claim is within the policy excess or the claim is in excess of the policy cap.[291] Most importantly, the value of the insurance can diminish in the insolvency of the data recipient, which is when it is most needed, as customers will not be able to be fully compensated by making a claim against an insolvent data recipient. Although there are statutory protections of the priority to insurance proceeds in an insured's insolvency,[292] it is still necessary that a claim arises and is made by the insured before the policy is cancelled. This is relevant because cancellation of the policy on the commencement of insolvency is a common occurrence.[293] For these reasons, professional indemnity insurance has been found to be an 'imperfect mechanism' to achieve protection for consumers in the context of compensation of retail financial services clients.[294] Similarly, professional indemnity insurance is unable to sufficiently guarantee the data recipient's creditworthiness to ensure that a customer will be compensated for a breach by the data recipient of its information security or other obligations.[295] This reliance on professional indemnity insurance to ensure that customers can be compensated for defaults by data recipients

288. *See PSR*, *supra* note 75, at reg. 18(4); In Australia, the ACCC contemplates both professional indemnity insurance and cyber insurance, but notes that the latter is often limited in nature. AUSTL. COMPETITION & CONSUMER COMM., SUPPLEMENTARY ACCREDITATION GUIDELINES – INSURANCE 4 (2020).

289. AUSTL. SEC. & INV. COMMISSION, RG 126: COMPENSATION AND INSURANCE ARRANGEMENTS FOR AFS LICENSEES ¶ RG126.23 (2020).

290. RICHARD ST. JOHN, AUSTL. GOVT., COMPENSATION ARRANGEMENTS FOR CONSUMERS OF FINANCIAL SERVICES (2012).

291. *Id.*

292. For example, the protection for third parties to which the insolvent has incurred the relevant liability. CORPORATIONS ACT 2001, Section 562 (Cth Austl.).

293. It is possible that the insolvency administrator may discontinue further premium payments on the policy on the basis that they can only benefit some of the insolvent's creditors. ST. JOHN, *supra* note 290, at 34; Insurance policies which continue after the insolvency of the insured are not generally available. AUSTL. COMPETITION & CONSUMER COMM., *supra* note 289, at ¶ RG126.11.

294. ST. JOHN, *supra* note 290.

295. "[C]ompensation arrangements, based largely on professional indemnity insurance, provide a measure of assurance, but no guarantee that retail clients will be able to recover compensation to which they may be entitled." *Id.* at 153.

creates a risk to be managed in open banking when compared to the benchmark of deposit protection in banking.

3. Summary

This part has analysed two foundations of customer's trust in data recipients – information security and customer compensation. It shows that the operational information security requirements in each framework are similar and are comparable with the approach taken in banking. It also shows that the requirements for insurance to compensate customers are also broadly comparable between the Australian and UK open banking. Further, it argued that the insurance requirements create risks to be managed when evaluated against the protection provided to customers by deposit protection. These risks could affect the trust which customers place in open banking and increases the exposure taken by customers on the performance by the data recipient of its responsibilities for shared data.

VII. Conclusion: Performance, Risk and Trust in Open Banking

This article has compared the legal responsibilities of data recipients for shared data under open banking in Australia and the United Kingdom. This comparison should be a valuable resource in establishing open banking in a new jurisdiction, such as the United States. In addition, this article has conducted an evaluation of those responsibilities under open banking against legal responsibilities for customer funds under banking law. This evaluation is intended to demonstrate how a jurisdiction's own banking law can be used as an important reference point in designing open banking's legal architecture. The analysis noted that some differences between open banking and banking laws, such as those relating to data minimization, customer consent and the integrity of customer data, are justifiable due to fundamental differences between customer data and customer funds arising because of data's non-rivalrous, non-excludable and non-fungible nature. However, these differences do not negate the similarities between the accountability functions performed with respect to customer data in open banking and customer funds in banking.

The functional similarity between the responsibilities in banking and open banking has been most clearly shown in the reliance on the performance of the recipient of the data or funds. The reliance placed on the compliance by the data recipient with its responsibilities in open banking this exposes customers to risk on the data recipient's performance. Customers are required to place trust in the performance of their data recipient without being able to verify that recipient is worthy of that trust through its performance. This represents a risk to be managed

in open banking because 'trustworthiness can often be ascertained only some considerable length of time after trust has been conferred.'[296]

Comparable performance risks, known as credit risks, arise in banking. Banks make promises to pay funds to customers to be performed at a later time. If these promises are not performed, then confidence in the bank can quickly collapse, resulting in a 'bank run' and a loss of confidence in the banking system as a whole.[297] The need to manage these risks is a key element of banking regulation.[298] However, some of these methods rely on money's fungibility and objective value. For example, the payment of amounts which are due can be verified, the obligation to pay can be collateralized by other amounts of the same value, and the payment obligations between parties can be simplified by clearing and settlement.[299] These methods are not applicable to open banking as data are neither fungible nor have an objective value, and because there is no settlement asset which can be delivered to customers to finally discharge the data recipient's obligations.[300] Nevertheless, other aspects of the management of credit risk in banking could be considered to manage the performance risks in open banking particularly as it develops. First, data recipients could monitor and report the level of performance responsibilities which they are incurring, similar in concept to how credit risk is monitored in banking.[301] This would allow regulators to determine how much risk is being taken, particularly if a participant is showing signs of non-compliance.[302] Second, the design of open banking could ensure that compensation for customers who have suffered loss because of the failure of their data recipient is available even if the data recipient is insolvent, which is when such protection is likely to be most needed. Whilst it might take time to develop the insurance market to provide this, it would enable the performance of a similar function to depositor protection in banking,[303] and would support the confidence placed in open banking by 'providing advance protection against future deviant outcomes or compensation for accomplished misdeeds.'[304] Third, the technological means of enabling performance to be verified could be developed so that a function comparable to that of a settlement asset can be performed. This could involve standardising the

296. Susan P. Shapiro, *The Social Control of Impersonal Trust*, 93 AM. J. SOCIO. 623, 643 (1987).

297. *See supra* Part VI 2(b).

298. *See* ARMOUR ET AL., *supra* note 168.

299. *Id.*; *See also* GEVA, *supra* note 28.

300. *See supra* V 2(b); As a result, the concept of "settlement finality" which is so critical in payment systems is not operable in open banking frameworks. *See* COMM. ON PAYMENT & SETTLEMENT SYS. & INT' ORG. OF SEC. COMM'NS, *supra* note 272, at 64.

301. *See* COMM. ON PAYMENT & SETTLEMENT SYS. & INT' ORG. OF SEC. COMM'NS, *supra* note 272.

302. This concept is not dissimilar to the monitoring of credit risk taken by a clearing house in relation to its open positions. *Id.* at 42.

303. *Id.*

304. Shapiro, *supra* note 296, at 643.

nature of the legal responsibilities being incurred so that they can be coded into technological processes. It could also involve enabling the data shared to be technologically traced in a way which verifies performance. Whilst these might not be possible to implement in the short term, any increase in transparency would support the trust placed by customers in open banking.

It is important to note that the analysis in this article is narrow, focusing on the evaluation against responsibilities for customer funds under banking law. Accordingly, the need to manage performance risks which customers take on data recipients in open banking revealed should not be seen as justification for not implementing open banking. A broader perspective will quickly show that customers are exposed to greater performance risks when sharing data when they do not have the protection of the responsibilities imposed by open banking, even if those responsibilities are not the same as those applicable to their funds. Also, as important as these considerations are, this article does not argue that the legal responsibilities for transferred funds are the *only* benchmark which should be used in the design of responsibilities for shared data in open banking. Others include more general privacy and data protection laws. Nevertheless, for designing the legal architecture of open banking where it is not yet established, this article has shown that the principles of banking law are an important design tool available for the creation of the legal responsibilities which underpin the accountability at open banking's foundation, for the management of the risks which arise from non-performance of those responsibilities, and for establishing the trust with customers which is essential to open banking's success.