SCREEN SCRAPING IN AUSTRALIAN FINANCE

NATALIA JEVGLEVSKAJA * AND ROSS P BUCKLEY †

Millions of Australians give their online banking credentials to third parties so as to gain access to financial products and services enabled by the analysis of the data in their bank accounts. This practice of Screen Scraping ('SS') has contributed significantly to the rise of the FinTech industry. While the risks SS entails are significant, nowhere has the practice been formally outlawed despite the availability of safer data transfer arrangements under Open Banking regimes. We examine approaches to SS in the European Union, the United Kingdom and Australia, and argue that the practice should be prohibited here. Such a ban would have two salutary effects: it would protect consumers in financial hardship who use payday loans and it would accelerate uptake of the Consumer Data Right.

I INTRODUCTION

By 2017, when the Australian Government announced its intention to roll out an economy wide Consumer Data Right ('CDR'), over two million Australians were giving away their bank account login credentials to third parties.[1] These third parties 'scraped' data from a customer's internet banking interface and used it to offer financial products and services, in addition to, or in lieu of, the products and services offered by the customer's bank.[2] Colloquially known in finance circles as Screen Scraping ('SS'), this practice had boomed since 2001, when only perhaps 5000 Australians a year were using it.[3] SS gives businesses (mostly FinTechs) access to customer data without further identification vis-à-vis the account hosting bank and is now widely used globally. For example, as of 2021, more than 4 million Canadians — making up over 10 per cent of Canada's population — reportedly rely on financial services that employ SS technology.[4] In the US, the

* Research Fellow on the ARC Laureate Project entitled 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks' at UNSW Sydney.
† Australian Research Council Laureate Fellow and a Scientia Professor at UNSW Sydney.

1 FinTech Australia, Submission No 182 to Productivity Commission, *Inquiry into Data Availability and Use: Open Financial Data* (August 2016) 4 ('FinTech Submission'); Treasury (Cth), *Report of the Review into Open Banking: Giving Customers Choice, Convenience and Confidence* (Report, December 2017) ('*Review into Open Banking*') 51, 72.

2 *Review into Open Banking* (n 1) 51.

3 Australian Securities and Investments Commission, *Account Aggregation in the Financial Services Sector* (Consultation Paper No 20, May 2001) 19 ('*Account Aggregation*').

4 Advisory Committee on Open Banking, *Final Report* (Report, April 2021) 7.

DOI: 10.38127/uqlj.v42i2.7193

Financial Data Exchange ('FDX')[5] estimates that, as of 2020, data access and sharing for 65–85 million US consumers — 20–25 per cent of the population — was provided through shared customer login credentials.[6]

The advantages and downsides of commercial SS, aka 'digital data capture', have been thoroughly discussed.[7] Some regard it to be an outrageous practice that needs to be excised from finance as quickly as possible. Others maintain that SS enables delivery of novel products and services customers could not otherwise access.[8] Arguing that there is no evidence of consumer harm from SS, its proponents suggest the FinTech industry would be crippled should it be outlawed.[9] Banks accuse FinTechs of stealing their customers' data. FinTechs accuse banks of restricting access to information that should be controlled by customers.

Where SS is the only way to access customer data required for the provision of a service, opposition to a ban is, perhaps, understandable. If businesses reliant on data cannot access it, they cannot compete in the financial services market. However, competition, desirable as it is, should neither come at the expense of data safety and security nor facilitate exploitation of financially vulnerable members of our society.

Although the risks that SS entails for businesses and customers are real and serious, the practice has not been formally outlawed anywhere. Misconceptions abound that SS has been banned in Europe.[10] However, while the European Union ('EU') and United Kingdom ('UK') have commendably restricted the practice, it endures there, as we demonstrate. Jurisdictions that facilitate and regulate Open Banking and Open Finance, such as the EU, the UK, and Australia, expect SS to become redundant with the wider adoption of the Application Programming Interfaces ('APIs'), which underpin Open Banking and Open Finance and are a far safer mode of data transfer.[11] Yet, the rollout of Open Banking is slow and inertia powerful.

We argue that Australia should, when the timing is propitious, explicitly outlaw SS to protect consumers experiencing financial hardship from

---

5 Financial Data Exchange ('FDX') is a non-profit, industry standards body, dedicated to unifying financial services around a common, secure, and interoperable technical standard for user-permissioned sharing of financial data: see Financial Data Exchange 'About FDX', *Financial Data Exchange* (Web Page, 2023) <https://financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6>.

6 Financial Data Exchange, Comments to Consumer Financial Protection Bureau, *Consumer Access to Financial Records: Advanced Notice of Proposed Rulemaking* (2020) 9.

7 See Part IV, below.

8 For various sources that oppose but also those that support Screen Scraping ('SS'), see Part IV, below.

9 Senate Select Committee on Financial Technology and Regulatory Technology, Parliament of Australia, *Interim Report* (Report, September 2020) 145 [5.58], 146 [5.62], 152 [5.58] ('*Senate Select Committee Interim Report on Financial Technology and Regulatory Technology*').

10 See further n 40, below.

11 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 144 [5.54]; The Australian Government the Treasury, *Statutory Review of the Consumer Data Right* (Report, 2022) 31 <https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf>.

unscrupulous non-bank lenders and to accelerate the implementation of CDR. Without regulatory intervention there is a real risk that the costs of accreditation under the CDR regime, inertia and path dependence, and the lure of the inappropriate use of data that SS offers, will all combine to see this practice endure well past when it is in the interests of consumers and the broader economy.

The article is structured as follows. Part II examines the origins of SS. Part III explores the legal and regulatory frameworks in the EU and the UK, in general for context, and specifically to debunk the myth that SS is banned in these jurisdictions. We also consider the lack of enthusiasm of the Australian Government (until most recently) to proactively regulate SS in Part III.[12] Part IV examines the upsides and downsides of SS, and Part V the arguments for its prohibition. Part VI concludes.

II Screen Scraping: Origins and Evolution

Scraping data,[13] including financial data, goes back to the emergence of 'data aggregation', also known as 'account aggregation', in the late 1980s in the US.[14] A select few wealthy clients of some US banks are reported to have been benefitting from data accumulation features that allowed for an easy account review since as long ago as the 1980s.[15] As more data was increasingly captured digitally at lesser cost, a new industry sprang up to make a unique value proposition to consumers, namely to 'aggregate their financial lives onto one web site'.[16]

Typically, national banks ('aggregator banks') provided aggregation services under their brand name through third parties specialising in gathering, storing and presenting data to the customer ('data aggregators').[17] The data could range from information available publicly online (such as travel or store specials and

---

12 See also Part VB below.

13 Screen Scraping ('SS') has many names. It is also referred to as 'data scraping', 'web scraping', 'web harvesting', or 'data harvesting'.

14 See Julia Gladstone, 'Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data' (2001) 19(1) *Journal of Computer and Information Law* 313, 315. See also Jennifer Aguilar, 'The Data Dilemma: Regulating the Lifeblood of Fintech Innovation' *Business Law Today* (Web Page, 8 April 2021) <https://businesslawtoday.org/2021/04/data-dilemma-regulating-lifeblood-fintech-innovation/>. See also Don Cardinal and Nick Thomas, 'Data Access Technology Standards: A History of Open Banking Data Access' in Linda Jeng (ed), *Open Banking* (Oxford University Press, 2022) 91, 94. See also Michael Kitces, 'The Six Levels of Account Aggregation #FinTech Solutions and PFM Portals for Financial Advisors', *Kitces.com* (Blog Page, 9 October 2017) <https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/>.

15 Gladstone (n 14).

16 Kimberly Wierzel, 'If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions' (2001) 5(1) *North Carolina Banking Institute* 457, 465.

17 Office of the Comptroller of the Currency, 'Bank-Provided Account Aggregation Services: Guidance to Banks' *Office of the Comptroller of the Currency* (Bulletin, 28 February 2001) <https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html> ('*Guidance to Banks*'). See also Wierzel (n 16) 458.

real estate information), personal account information (including credit cards and deposit accounts),[18] to non-financial information (such as balances from frequent flyer or other reward programs or data from utility and insurance companies).[19] To access personal information, aggregators relied on customer-provided usernames and passwords. To benefit from the service, a customer had to nominate websites and the information to be collected therefrom and share their user credentials for each. The advantage for the customer was obvious: they could access all of their nominated financial and other information in one place and needed to remember only *one* username and password.[20]

Banks were eager to offer account aggregation solutions to increase the usefulness of their banking services to customers. They saw it as an opportunity to leverage their position as trusted (financial) intermediaries and thus deepen their customer relationships.[21] Most importantly, banks soon realised that the choice for them may be 'either to aggregate or be aggregated', as the prospect of losing their customers to an aggregation service provided by a competing financial institution was real and daunting.[22] Furthermore, because data aggregation facilitated an overview of businesses the customer was using and consequently offered new marketing opportunities, independent account aggregation services soon penetrated the market with commercial propositions with which banks struggled to compete.[23]

Before long, the business model of account aggregation via data scraping spread to Australia and other jurisdictions, including South Korea, Japan, and Europe.[24] The Australian Securities and Investment Commission ('ASIC') reported that seven account aggregation service providers were operating here by April 2001: two financial institutions, a stockbroker, a retail web-portal and two other businesses.[25] Marketing campaigns emphasised numerous benefits for consumers, above all the more efficient management of personal finances.[26]

---

18 *Guidance to Banks* (n 17). See also Federal Financial Institutions Examination Council, 'E-Banking, IT Examination Handbook' (Handbook, August 2003) appendix D, D-1.

19 *Account Aggregation* (n 3) 7.

20 Ibid 9.

21 *Guidance to Banks* (n 17). See also Office of the Comptroller of the Currency, 'OCC Issues Guidance on Bank-Provided Aggregation Services' (News Release, 2 March 2001) <https://www.occ.gov/news-issuances/news-releases/2001/nr-occ-2001-22.html>.

22 See Gladstone (n 14) 314. See also Jeffrey Hirschey, 'Symbiotic Relationships: Pragmatic Acceptance of Data Scraping' (2014) 29 *Berkeley Technology Law Journal* 897, 921.

23 Gladstone (n 14) 315–16. See also Julie Williams, 'The Impact of Aggregation on the Financial Services Industry' (Speech, American Banker's 2nd Account Aggregation Conference, 23 April 2001).

24 While account aggregation could also be done via 'direct feed arrangement' with the financial institution hosting the data (ie, Application Programming Interfaces), this method was considered costly and time-consuming and, consequently, less attractive for aggregators. See *Account Aggregation* (n 3) 2, 15, 18, 21; Hiroshi Fujii et al, 'E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific' (Working Paper No 2002-06, Massachusetts Institute of Technology, September 2002) 2.

25 *Account Aggregation* (n 3) 17.

26 See Jessica Aldred, 'Ninemsn Launches Account Master', *Internet News* (online, 11 December 2000) <https://www.internetnews.com/it-management/ninemsn-launches-account-master/>.

Indeed, over time many areas of social activity have come to rely on data scraping: internet auctions,[27] search engines (Google, Bing, Yandex, etc), airline, vehicle and holiday-housing price aggregation,[28] targeted advertising,[29] website preservation,[30] academic research,[31] journalism,[32] and many more.[33] Data scraping has become an important part of providing 'user convenience' and saving time.

In the financial sector, data aggregators expanded their operational systems and moved to selling data-access services to a growing number of FinTechs who did not have capacity to collect the data themselves, but who, armed with that data, could potentially challenge the incumbents in the provision of financial products and services.[34] Today, companies that utilise SS for data aggregation do so for a range of reasons and use cases. Some access customers' bank accounts on an ongoing basis to provide investment products or financial management tools; others access account information on a one-off basis, for example, to view transaction records as part of a loan assessment process.[35]

Two business models have emerged. SS can be undertaken by a FinTech offering the underlying service, such as a personal finance management tool

---

27 Trevor Jeffords, 'What Is "Screen Scraping" and Is It Lawful in Australia?' (2001) 12 *Computers and Law* 24. See also Michael Schrenk, *Webbots, Spiders, and Screen Scrapers* (No Starch Press, 2nd ed, 2012) 323.

28 Expedia, Orbitz, Kayak, Skyscanner, Booking.com, etc.

29 Sergey Ermakovich, 'How to Use Web Scraping for Marketing and Product Analytics', *Venturebeat* (online, 8 April 2022) <https://venturebeat.com/2022/04/08/how-to-use-web-scraping-for-marketing-and-product-analytics/>.

30 Adrian Brown, *Archiving Websites: A Practical Guide for Information Management Professionals* (Facet Publishing, 2006) 50-9. See also Digital Preservation Coalition, 'Preserving the Web' (Note, 13 September 2018) <https://www.dpconline.org/docs/knowledge-base/1861-dp-note-10-preserving-the-web/file>; Library of Congress, 'Saving the World Wide Web' (Web Page) <https://www.digitalpreservation.gov/series/challenge/web_harvest_challenge.html>.

31 Alex Luscombe, Kevin Dick and Kevin Walby, 'Algorithmic Thinking in the Public Interest: Navigating Technical, Legal, and Ethical Hurdles to Web Scraping in the Social Sciences' (2022) 56 *Quality and Quantity* 1023, 1024; Geoff Boeing and Paul Waddell, 'New Insights into Rental Housing Markets across the United States: Web Scraping and Analyzing Craigslist Rental Listings' (2016) 37(4) *Journal of Planning and Education and Research* 457, 459.

32 Rachel Goodman, 'Tips for Data Journalism in the Shadow of an Overbroad Anti-Hacking Law', *American Civil Liberties Union* (online, 13 October 2017) <https://www.aclu.org/news/privacy-technology/tips-data-journalism-shadow-overbroad-anti-hacking-law>. See also Nael Shiab, 'On the Ethics of Web Scraping and Data Journalism', *Global Investigative Journalism Network* (online, 12 August 2015) <https://gijn.org/2015/08/12/on-the-ethics-of-web-scraping-and-data-journalism/>.

33 See Han-Wie Liu, 'Two Decades of Laws and Practice around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment' (2020) 30(1) *Washington International Law Journal* 28, 29; Andrew Sellars, 'Twenty Years of Web Scraping and the Computer Fraud and Abuse Act' (2018) 24 *Boston University Journal of Science and Technology Law* 372, 374.

34 However, banks still use SS too: see *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) [5.57]. See also Andres Wolberg-Stok, 'Open Banking Ecosystem and Infrastructure: Banking on Openness' in Linda Jeng (ed), *Open Banking* (Oxford University Press, 2022) 13, 17.

35 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) [5.48]–[5.49].

('PFM').[36] A customer will share her banking credentials with such a FinTech so it can retrieve her financial data from her bank, which the FinTech then typically stores along with the customer's ID and password in its database.[37]

The more common model, however, is where FinTechs use one of a small number of companies specialising in data aggregation to act as an intermediary between the FinTech and the customer.[38] This model limits the number of parties needing to hold a customer's credentials and include Plaid, Envestnet | Yodlee, Finicity, MX and others. These entities connect to financial institutions hosting customer accounts and collect, package and deliver the customer data to the FinTech.[39] This enables the FinTech to focus its time and resources on the development of core products and services.

III Legal Frameworks

The frequency and certainty with which industry and consumer rights organisations assert that SS has been generally outlawed in the EU and the UK is striking, given how wrong this assertion is.[40] While most expert commentary rightly observes that restrictions are limited to payments, it often fails to differentiate between the three constitutive components of conventional SS

---

36 Personal finance management ('PFM') tool is a software application that helps its users to manage their financial activities. PFM solutions range from transaction analysis and spending categorisation to personalised insights and recommendations, such as on savings or investments. See, eg, 'PFM Solutions for Banks', *Moneythor* (Web Page, 1 April 2021) <https://www.moneythor.com/2021/04/01/pfm-solutions-for-banks/>.

37 Financial Data Exchange, 'ABCs of the APIs' (Organization Overview, Financial Data Exchange, 2021) 3–5.

38 Ibid 3–4.

39 *Review into Open Banking* (n 1) 73; FinTech Submission (n 1) 4; Nizan Packin, 'Show Me the (Data about the) Money!' [2020] (5) *Utah Law Review* 1297. See also Rebecca Ayers and Suman Bhattacharyya, 'Why Screen Scraping Still Rules the Roost on Data Connectivity', *Envestnet Yodlee* (Blog Post, 18 June 2021) <https://www.yodlee.com/why-screen-scraping-still-rules-roost-data-connectivity>.

40 'Screen scraping has already been banned in the UK and Europe under Strong Customer Authentication rules': Julian Bajkowski, 'Screen Scraper Ban Touted to Weed out Data Predators', *ITNews* (online, 15 January 2020) <https://www.itnews.com.au/news/screen-scraper-ban-touted-to-weed-out-data-predators-536516>; 'Screen scraping has been banned in the UK and it's difficult to see the practice being allowed to continue in Australia for much longer once Open Banking is more mature': Den Burykin, 'Open Banking Pushback Shows Consumers Need Guidance', *Finextra* (online, 9 May 2022) <https://www.finextra.com/blogposting/22258/open-banking-pushback-shows-consumers-need-guidance>; '[U]nlike in the UK where screen scraping was first banned, it is still legal in Australia': Adatree, *Uncovering the Differences between Open Banking and Screen Scraping* (Report) <https://adatree.com.au/screen-scraping-open-banking-report#:~:text=Unlike%20screen%20scraping%2C%20Open%20Banking,these%20purposes%20than%20screen%20scraping.>. 'The Bank … suggests that the Inquiry examine if a ban on screen scraping … as has been introduced in the United Kingdom would support the financial sector's transition away from the practice': Reserve Bank of Australia, Submission to Treasury (Cth), *Inquiry into Future Directions for the Consumer Data Right* (23 April 2020) 3; 'Screen scraping has been banned in the UK and the EU under the Payment Services Directive 2 (PSD2)': Financial Rights Legal Centre and the Consumer Action Law Centre, Submission No 36 to Senate Select Committee, *Inquiry into Financial Technology and Regulatory Technology* (September 2019) 18.

practice, namely accessing customer account credentials, the technical process of 'scraping' data from the customer-facing online interface, and the impersonation of the customer.[41] The elements of impersonation and credential sharing are of most concern to the opponents of SS.[42] Only the element of impersonation, however, is no longer tolerated by the EU and the UK's frameworks, with the other two elements remaining, as is shown below. Importantly, in certain circumstances all three components of 'traditional' SS can no longer be employed. As we will demonstrate, where a bank has implemented a compliant, stress-tested, and widely-used API it can be exempt from the duty to establish a contingency mechanism under which customer data is accessed through 'conventional' SS. The value of this restriction remains significantly constrained, however, by its limitation to payment accounts.

This Part first examines legal and regulatory frameworks on the sharing of customer financial data in the EU and the UK and then discusses the stance on SS of the Australian government.

A *The EU Framework*

In the EU, Directive 2015/2366 on payment services in the internal market ('*PSD2*')[43] mandated the move to 'Open Banking' by creating a digital environment that enables customers to consent to third parties accessing their payment account information or making payments on their behalf.[44] Seeking to promote competition and innovation in the EU and EEA payment sectors, the Directive opened them to a range of Payment Service Providers ('PSPs'), including non-bank entities — FinTechs — that offer consumer- or business-oriented payment services based on access to data from payment accounts.[45] Two new categories of such services were regulated and harmonised under PSD2: Account

---

41 See, eg, John Casanova and Max Savoie (eds), *Payment Services, Law and Practice* (Edward Elgar Publishing, 2022) 29. For correct and comprehensive analysis, see Han-Wei Liu, 'Shifting Contour of Data Sharing in Financial Market and Regulatory Responses: The UK And Australian Models' (2021) 10(3) *American University Business Law Review* 287, 294.

42 See Part IVA, below.

43 *Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC* [2015] OJ L 337 ('*PSD2*'). *PSD2* came into force on 12 January 2016 (replacing an earlier regulation from 2009). It had to be transposed into national legislation by 13 January 2018: see art 115(1). On national transposition, see *National Transportation Measures Document 32015L2366* [2018].

44 While there is no one definition of Open Banking, from the European perspective, Open Banking, at a minimum, includes products and services based on the sharing of 'payment account data' as mandated by *PSD2* (n 43). See, eg, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* [2020] COM 66, 30.

45 Payment Service Providers ('PSP') is a broad term that includes banks and third parties providing selected financial services, including AIS and PIS: see *PSD2* (n 43) arts 1, 4(11), annex I. See also European Banking Federation, 'Guidance for Implementation of the Revised Payment Services Directive' (PSD2 Guidance, EBF, 20 December 2019) 6.

Information Services ('AIS') and Payment Initiation Services ('PIS'),[46] respectively offered by Account Information Service Providers ('AISPs'), and Payment Initiation Service Providers ('PISPs').[47]

AIS collect and consolidate data from a customer's online payment accounts held with multiple Account Servicing Payment Service Providers ('ASPSPs')[48] — usually banks — in a single place allowing her to better manage personal finances by analysing spending patterns and financial needs in a user-friendly manner.[49] Companies such as Mint in the US, Money Dashboard in the UK, and Frollo[50] in Australia are all now leading brands in this field.

Sofort in Germany and iDeal in the Netherlands pioneered business models in PIS. These payment services radically simplified online payments by acting as a 'bridge' between the customer's financial institution and the merchant's account.[51] Instead of using a credit card and paying credit card fees or going through the hassle of logging into their bank account and then filling in the recipient's account details and other information required for the purchase, the customer can have a facilitator initiate a payment from their account to a payee's account.[52] With PIS, the customer only needs to authenticate with their bank, select the preferred account and confirm a payment order directly through the service she is using.[53]

The permissibility of SS by AISPs and PISPs became a subject of heated debate during the drafting of Regulatory Technical Standards ('RTS') under art 98(1) *PSD2*. These standards lay out specific requirements on secure authentication and communication between different actors in the *PSD2* payment ecosystem.[54] Charged with their development, the European Banking Authority

---

46 As defined in *PSD2* (n 43) arts 4(16) and 4(15) respectively.

47 As defined in *PSD2* (n 43) arts 4(18), 66, 4(19), 67 respectively. See also UK Finance, 'PSD2 Guidance: Open Access Guidance for Account Servicing Payment Service Providers' (Guidance, April 2020) [1.1].

48 For a definition of Account Servicing Payment Service Providers ('ASPSP'), see *PSD2* (n 43) art 4(17).

49 *PSD2* (n 43) Preamble, recital 28.

50 In July 2020, Frollo has been acquired by NextGen.Net, Australian market leader and innovator in lending technology: see Frollo, 'NextGen.Net Acquires Frollo to Lead the Way in Open Banking', (Blog Post, 7 July 2020) <https://frollo.com.au/blog/nextgen-acquires-frollo/>.

51 Gabriella Gimigliano, 'Title III, Chapter 2, "Authorisation of Payment Transactions" (Arts 64–77)' in Gabriella Gimigliano and Marta Božina Beroš (eds), *The Payment Services Directive II: A Commentary* (Edward Elgar, 2021) 146, 157 [9.036].

52 For illustration on how payment initiation through Sofort and iDeal works, see, eg, Sofort UK Ltd, 'Pay with Sofort', *Sofort* (Web Page, 2023) <https://www.sofort.com/pay-with-sofort/>; Sofort GmbH, 'SOFORT: Direct Payment via Online Banking' (Youtube, 18 August 2015) <https://www.youtube.com/watch?v=Tt-tN0944pE>; iDeal, 'What is iDeal?'(Web Page, 2023) <https://www.ideal.nl/en/consumers/what-is-ideal/>.

53 See 'Payment Services Directive: Frequently Asked Questions', *European Commission* (Web Page, 12 January 2018) <https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_5793>. See also Tink AB, 'What Is Payment Initiation, and What Is It Good for?', *Tink* (Web Page, 1 October 2020) <https://tink.com/blog/open-banking/what-is-payment-initiation/>.

54 *Commission Delegated Regulation (EU) 2018/389 Supplementing Directive (EU) 2015/2366 of the European Commission and of the Council with regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication* OJ L69/23 ('*RTS*'). 54

('EBA'), was inclined to ban SS.[55] However, the final decision-making power on the adoption of the standards was vested in the European Commission,[56] which — in response to industry concerns — allowed for several indirect means by which SS could continue. Specifically, from the date the RTS came into effect, ASPSPs had to enable access to customer accounts via one of the authorised methods: either a 'dedicated interface' or a modified version of the customer interface that meets the requirements of RTS.[57] Seeking to ensure technology and business-model neutrality, *PSD2* does not prescribe specific technologies or standards.[58] For dedicated interfaces, however, ASPSPs have generally regarded APIs as the preferred technology.

A modified customer interface refers to an online banking interface originally devised for authenticating and communicating with the ASPSPs' users (ie banks' customers) but modified in a way that would allow an AISP or PISP to identify itself to the financial institution operating the account.[59] Qualified certificates for electronic seals or qualified certificates for website authentication, commonly referred to as e-IDAS certificates, must be used for identification.[60] Such certificates should include all the information an ASPSP needs to identify an AISP or PISP and determine its authorisation status.[61] Accessing data through an adjusted customer interface created an opportunity to use SS in a new, modified form and is occasionally referred to as 'screen scraping plus' ('SS plus').[62] This is the point that is often overlooked: an AISP or PISP may still legitimately rely on a customer's personalised security credentials to employ automated methods of

---

55 *PSD2* (n 43) art 98(1); European Banking Authority, *Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)* (Report No EBA/RTS/2017/02, 23 February 2017) 4. See also European Banking Authority, 'Opinion of the European Banking Authority on the European Commission's Intention to Partially Endorse and Amend the EBA's Final Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under *PSD2* EBA/Op/2017/09' (Opinion, 29 June 2017) 8.

56 *PSD2* (n 43) arts 98(4), 10–14.

57 *RTS* (n 54) arts 30–1.

58 *PSD2* (n 43) art 98(2)(d).

59 *RTS* (n 54) preamble para 20 and art 30(1).

60 See *RTS* (n 54) art 34(1); *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC* [2014] OJ L 257/73, arts 3(30), 3(39). On e-IDAS generally, see Douglas W Arner et al, 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities' (2019) 20(1) *European Business Organisation Law Review* 66, 68.

61 UK Finance (n 47) 7–8.

62 Ibid 16 [8.5]; Arab Regional Fintech Working Group, 'Open Banking Regulatory Principles' (Report No 164, Arab Monetary Fund, March 2021) Annex. See also Adam Polanowski and Przemysław Gruchała, 'Can a User's Account Be Accessed Through Screen Scraping?', *Newtech.law* (online, 15 March 2019) <https://newtech.law/en/can-a-users-account-be-accessed-through-screen-scraping/>.

'scraping' data, even though an AISP or PISP can no longer 'impersonate' the customer holding the account.[63]

Another backdoor means of SS that *PSD2* opened are the 'contingency measures' under art 33 that an ASPSP must take establishing a dedicated API. The contingency mechanism requirements are intended to ensure an AISP or PISP can access customer data through the online interface the customer has with their ASPSP in the event an API does not perform as required, or becomes unavailable (ie unplanned downtime), or when the system breaks down.[64] Compared to the practice of SS prior to *PSD2*, impersonation of the customer is no longer allowed when a contingency mechanism is triggered; an AISP/PISP must be able to identify itself towards the ASPSP.[65] However, the other two elements of 'traditional' SS — ie credential sharing and automated process of capturing data from user interfaces — remain intact under *PSD2*.[66]

An exemption from the obligation to adopt contingency measures may be granted by national authorities where an ASPSP has implemented an RTS compliant, stress-tested API used extensively for at least three months.[67] In such a scenario, an AISP or PISP would be barred from using SS technology in relation to customer payment accounts held by an exempted ASPSP.

B *The UK Framework*

The legal foundation for the UK Open Banking framework is formed by pt 2 of the *Retail Banking Market Investigation Order 2017* ('*CMA Order*')[68] and pt 7 of the *Payment Services Regulation* ('*PSR*'),[69] which translated *PSD2* into UK legislation. The *CMA Order* established an Open Banking Implementation Entity ('OBIE') to create standards for data sharing (UK Open Banking Standards).[70] These standards were required to cover APIs, data formats, and security as well as governance arrangements and customer redress mechanisms,[71] and to not

---

63 Ruth Wandhöfer, 'Title IV, Chapter 5 "Operational and Security Risks and Authentication" (Arts 95–98)' in Gabriella Gimigliano and Marta Božina Beroš (eds), *The Payment Services Directive II: A Commentary* (Edward Elgar, 2021) 190, 200 [12.076]. See also PTJ Wolters and BPF Jacobs, 'The Security of Access to Accounts under the PSD2' (2019) 35(1) *Computer Law and Security Review* 29, 36–7.

64 *RTS* (n 54) art 33(1).

65 Ibid art 33(5).

66 UK Finance (n 47) 7–8.

67 *RTS* (n 54) art 33(6). See also European Banking Authority, 'Guidelines on the Conditions to Benefit from an Exemption from the Contingency Mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)' (Final Report No EBA/GL/2018/07, European Banking Authority, 4 December 2018).

68 *Retail Banking Market Investigation Order 2017* (UK) ('*CMA Order*'). The order is made under the *Enterprise Act 2002* (UK) ('*Enterprise Act*').

69 *Payment Services Regulation 2017* (UK) ('*PSR*').

70 *CMA Order* (n 68) art 10.1.

71 Ibid (n 61) art 10.2. See also Open Data Institute and John Fingleton, *Open Banking, Preparing for Lift Off* (Report, July 2019) 23.

'include provisions that are incompatible with the requirements in *PSD2*'.[72] The *PSR* imposes data-sharing obligations on 'account servicing payment service providers' ('ASPSP)' — ie data holders or banks — with respect to requests made by AISPs and PISPs — ie accredited data recipients.[73]

Regulations 69(2)(a) and 70(2)(a) of the *PSR* mandate that ASPSPs must comply with RTS, which also provide the basis on which the UK Open Banking Standards are approved for compliance with the *PSR* for a UK bank. The backdoors to SS have thus been entrenched in the UK's regulatory framework as a rule.[74] Since 14 September 2019,[75] AISP or PISP access to customer payment account information had to be enabled via either a dedicated interface or a modified version of the customer interface that meets the requirements of RTS.[76] Where an ASPSP chooses to provide access via a dedicated interface, it must have contingency measures in place. An exemption from the obligation to provide a contingency mechanism can be granted by the Financial Conduct Authority ('FCA') — the regulator of the UK Open Banking framework — to a financial institution showing it has implemented an RTS compliant, stress-tested, and widely-used API.[77] Thus, unless the financial institution holding customer data has established open API channels and is exempt from the duty to provide for a contingency mechanism, an AISP or PISP can access customer data using customer credentials and SS technology, provided it identifies itself towards the ASPSP.

C *Limitations of the EU and the UK Frameworks*

Both the EU's and the UK's frameworks remain limited in one significant respect, which may retain the attractiveness of and, arguably, even the need for SS. *PSD2* is focused on payment accounts[78] and applies to payment services provided within the EU and EEA. The UK framework is similarly limited to payment systems. The *CMA Order* requires access to be given to transaction information for

---

72 *CMA Order* (n 68) art 10.2.

73 *PSR* (n 69) rr 2, 69–70.

74 Financial Conduct Authority, 'Payment Services and Electronic Money: Our Approach' (Report, November 2021) 234ff.

75 Note, however, that due to a range of technical challenges faced by industry in implementing different *RTS* requirements, the Financial Conduct Authority has shifted the deadline for the full compliance with *RTS* several times with the most recent date being set to 30 September 2022: see Financial Conduct Authority 'Strong Customer Authentication', *Financial Conduct Authority* (Web Page, 15 February 2023) <https://www.fca.org.uk/firms/strong-customer-authentication>.

76 Specifically, articles 30 and 34-36: see Financial Conduct Authority (n 74) 235.

77 Ibid 236.

78 A payment account is defined in article 4(12) of *PSD2* as 'an account held in the name of one or more payment service users which is used for the execution of payment transactions'. 'The RTS only covers payment accounts in the scope of PSD2': see also European Commission, 'Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) Enabling Consumers to Benefit from Safer and More Innovative Electronic Payments' (Memo, 27 November 2017).

personal current account products[79] and business current account products.[80] The *PSR* adds to this list the requirement to give access to data from a 'payment account', ie 'an account held in the name of one or more payment service users which is used for the execution of payment transactions'.[81] In the view of the FCA, payment accounts include 'current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account mortgages.'[82] Mortgage and loan accounts, fixed-term deposit accounts and cash-savings accounts are not subject to the UK framework.[83]

Even where the exchange of customer payment account data between a bank and a FinTech runs well via an API, it provides only partial insight into a customer's overall financial situation. As a consequence (unless a data holder provides access to other customer accounts beyond the PSD2 mandate), businesses offering, for example, consumer loans will not be able to access the information on customers savings and investment habits, unless they resort to SS, which offers visibility of all data held in the online banking channel.[84]

In short, as a matter of law, the prohibition of SS in the EU and the UK is limited to accessing *payment* account data *without* identification toward the account holding institution. Even though a closer inspection of payment accounts may reveal *some* data on the existence of and the amount of outgoings to other accounts, such as loan or mortgage accounts, these insights will always be partial and as such do not affect the scope of the limitation. In practice, the requirement of authentication is only extended to scenarios where data is scraped from non-payment accounts, such as savings or mortgage accounts, in a way that inadvertently captures data from payments accounts.[85] Accessing payment account data via SS *upon identification* towards the ASPSP remains lawful in both jurisdictions. Finally, *PSD2* contains no sunset clause either for the requirement to provide a modified customer-facing interface, or for 'contingency measures' under art 33 *PSD2*, suggesting the hybrid model of accessing customer data is

---

79 Including personal current accounts (with or without an overdraft facility), basic bank accounts, packaged accounts, reward accounts, student or graduate accounts and youth accounts: *CMA Order* (n 68) art 12.4.1.

80 Including business current accounts and 'standard tariff unsecured business overdrafts': *CMA Order* (n 68) art 12.4.2.

81 *PSR* (n 69) s 2.

82 Financial Conduct Authority (n 74) 213.

83 Ibid. See also Financial Conduct Authority, *FCA Handbook* (Financial Conduct Authority, 2013) PERG [15.3].

84 Ayers and Bhattacharyya (n 39); Nilixa Devlukia, 'PSD 1, 2, 3: We Are out of the Starting Blocks with a Marathon Ahead', *The Papers* (Blog Post, 27 July 2022) <https://thepaypers.com/expert-opinion/psd-1-2-3-we-are-out-of-the-starting-blocks-with-a-marathon-ahead--1257721>.

85 European Banking Authority 'EBA Responses to Issues XIV to XX Raised by Participants of the EBA Working Group on APIs under PSD2' (Document, 26 July 2019) <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/09da22b1-19a8-4538-949b-3eb4e28ded2e/Fourth%20set%20of%20issues%20raised%20by%20EBA%20WG%20on%20APIs.pdf?retry=1>.

likely to remain for now.[86] Importantly, both jurisdictions are yet to regulate SS in relation to non-payment accounts. As a matter of practice, PISPs and AISPs may need to accommodate different access methods — APIs for payment accounts and customer-facing user interfaces for non-payment accounts — unless ASPSPs equally offer (open) API access to the latter.

Whether a review of PSD2 will change the existing state of affairs remains to be seen. In May 2022, the European Commission commenced a consultative process to assess whether *PSD2* remains fit for purpose or needs revision. In June 2023, the European Commission ('EC') published its proposals for a new regulation intended to replace PSD2 — the Payment Services Regulation ('EU PSR') — and a new directive that focuses specifically on the licensing and authorisation of payment and e-money institutions ('*PSD3*').[87] While the proposed EU PSR places a stronger emphasis on the ASPSPs' obligation to provide dedicated interfaces (ASPSPs shall have in place *at least one dedicated interface* for the purpose of data exchange with AISPs and PISPs)[88] and establishes minimum standards for availability and performance of open banking APIs,[89] it nonetheless allows AISPs and PISPs to access payment accounts data via an interface that the ASPSPs use for authentication and communication with their users where dedicated interfaces become unavailable, thus leaving a backdoor for the use of SS upon identification towards the ASPSP.[90] One should also bear in mind that, regardless of the review outcome, the UK's departure from the EU means the relevance of the EU legislation to the UK framework will diminish and the UK Open Banking framework will continue developing on its own terms.[91]

D *Consumer Data Right*

Customer-data sharing in Australia is governed by the Consumer Data Right ('CDR') framework, which was established under the *Treasury Laws (Consumer*

---

86 TrueLayer notes that the contingency mechanism 'remains heavily used in some EU markets where bank APIs are still not functioning well': TrueLayer 'Response to Statutory Review of the Consumer Data Right' (Document, 20 May 2022) 23 <https://treasury.gov.au/sites/default/files/2022-09/c2022-314513-truelayer.pdf>.

87 As mandated under *PSD2* (n 43) art 108. See also *Proposal for a Regulation of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Regulation (EU) No 1093/2010* and *Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC*.

88 *EU PSR*, art 35(1) (emphasis added).

89 *EU PSR*, arts 35(3) and 36.

90 *EU PSR*, preamble para 57 and art 38. See also Sigrid Hansen, 'New draft Payment Services Regulation: Overview of the Main Differences from PSD2', *EY* (Web Page, 29 June 2023) <https://www.ey.com/en_be/financial-services/new-draft-payment-services-regulation-overview-main-differences-from-psd2>.

91 The UK formally ceased to be a member state of the EU on 31 January 2020 with the transition period ending on 31 December 2020. '[I]t is intended that the PSD II will eventually be replaced by Open Banking after Brexit': Victoria Dixon (ed), *Goode on Payment Obligations in Commercial and Financial Transactions* (Sweet & Maxwell, 4th ed, 2020) [5]–[77].

Data Right) Act 2019 (Cth) ('*CDR Act*').[92] The CDR differs fundamentally from other data-sharing regimes — including in the EU and the UK — in two fundamental respects: (i) it is not limited to sharing of payment account data and extends to other financial accounts,[93] and (ii) most importantly, it is designed to apply across many sectors of the economy. Initially rolled out in banking (where CDR is referred to as 'Open Banking'), the regime has been extended to the energy and telecommunications sectors, as well as to non-bank lenders.[94] An earlier decision to extend the CDR to 'open finance' — including superannuation and general insurance — has, however, been recently put on hold to allow the CDR time 'to mature', to allow the improvement of the quality of CDR data and also to ensure that the existing framework is functioning as efficiently as possible.[95]

The CDR statutory framework includes four core components: (i) the *CDR Act* as enabling legislation; (ii) CDR Designation Instruments issued under Part IVD of the *CDR Act*, which designate sectors of the Australian economy for the purposes of the CDR; (iii) CDR Rules; and (iv) Consumer Data Standards.

The *CDR Act* created a new Part IVD of the *Competition and Consumer Act 2010* (Cth) ('*CCA*'),[96] which outlined the overarching objectives and principles of CDR, set out the role and functions of the regulatory bodies charged with establishing and enforcing CDR rules, enshrined minimum privacy protections and empowered the Treasurer to apply CDR to economy sectors.[97] As mentioned, sector designation occurs through CDR Designation Instruments. For example, the *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (Cth) designated the banking sector.[98] Then, the CDR Rules regulate the scope of data to be shared within a designated sector and the circumstances in which data sharing is required, ie in response to a valid consumer request and subject to

---

92 *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) ('*CDR Act*').

93 Such as savings accounts, call accounts, term deposits, cheque accounts, debit card accounts, mortgage offset accounts, personal loans, trust accounts, foreign currency accounts, and others: see Australian Competition and Consumer Commission, 'Consumer Data Right: Phasing' (Document, December 2020) <https://www.accc.gov.au/system/files/20-64FAC_CDR_Phasing_D07.pdf>.

94 Note, however, that the implementation of the CDR in the telecommunications sector has been paused in mid-2023, to allow the regime to mature in finance and energy first. See Consumer Data Right, 'Consumer Data Right Newsletter' (26 May 2023) *Consumer Data Right Updates.*

95 *Consumer Data Right (Energy Sector) Designation 2020* (Cth); *Consumer Data Right (Telecommunications Sector) Designation 2022* (Cth); *Consumer Data Right (Non-Bank Lenders) Designation 2022* (Cth). See also Consumer Data Right, 'Consumer Data Right Newsletter' (26 May 2023) *Consumer Data Right Updates*; Australian Government, *Government Statement in Response to the Statutory Review of the Consumer Data Right* (Government Response, June 2023) 8 ('*Government Statement*'). See further The Australian Government the Treasury, 'Strategic Assessment: Outcomes' (Report, Treasury, January 2022) 1 ('*Strategic Assessment*'). See also Productivity Commission, *Superannuation: Assessing Efficiency and Competitiveness* (Inquiry Report No 91, 21 December 2018) 40. On Open Finance developments in the EU and the UK, see Ross P Buckley, Natalia Jevglevskaja, and Scott Farrell, 'Australia's Data Sharing Regime: Six Lessons for Europe' (2022) 33(1) *King's Law Journal* 28, 30.

96 *Competition and Consumer Act 2010* (Cth) ('*CCA*').

97 The Australian Government the Treasury, 'Consumer Data Right Overview' (Booklet, September 2019) 9 <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> ('CDR Booklet').

98 *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (Cth).

consumer consent.[99] The rules also set out privacy safeguards and regulate the use of data.[100] Finally, Consumer Data Standards stipulate the technical requirements by which data needs to be provided to consumers and accredited data recipients ('ADRs') within the CDR system.[101] Indeed, many aspects to handling CDR data require standardisation under the framework: the format and description of CDR data; the collection, use, security and disclosure of CDR data; the process for obtaining and withdrawal of authorisations and consents; consumer experience data standards, and many others.[102]

No explicit prohibition on SS is contained in the CDR framework. It does not include an obligation on data holders to establish a modified customer interface or ensure availability of a 'fallback mechanism' in the event dedicated interfaces fail to work as intended or experience a downtime.

The CDR's silence on SS was its drafters' deliberate choice back in 2017, when the government commissioned the Review into Open Banking in Australia to identify the most appropriate model for the national market and recommend the regulatory framework under which it would operate.[103] After considering a series of submissions that focused on the risks and opportunities presented by SS, the review found that SS had become the FinTech industry's default way of gaining authorised access to customer's financial data given that data sharing agreements with banks that would allow FinTechs to receive customer data via secure portals, such as dedicated interfaces, were, at best, few and far in between.[104] Crucially, the review concluded that Open Banking should neither endorse nor prohibit SS — as banning SS would remove an important market-based check on its design — but should aim to make the practice of SS redundant by facilitating a more efficient data-transfer mechanism.[105]

Subsequently, several significant consultative processes also turned their attention to the question of SS. In 2020, both the Senate Select Committee on Financial Technology and Regulatory Technology[106] (later renamed as the 'Select

---

99 See *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) ('*CDR Rules*'). Under CDR, 'consumers' include both individuals and businesses entities: see *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) s 56AI(3) ('*CDR Act*'); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 [1.100], [1.101].

100 *CDR Rules* (n 99) Part 7. See also Treasury, 'Statutory Review of the Consumer Data Right' (Issues Paper, March 2022) 4.

101 Ibid.

102 *CCA* (n 96) s 56FA(1). See also *CDR Rules* (n 99) r 8.11 and Part 8. For detailed information on these standards, see Data Standards Body, *Consumer Data Standards V1.23* (Electronic Standards) <www.consumerdatastandards.gov.au>.

103 *Review into Open Banking* (n 1) 121–2.

104 Ibid 72.

105 Ibid x, 72, 84.

106 The Committee was tasked to inquire into and report on the opportunities for Australian consumers and business arising from financial technology ('FinTech') and regulatory technology ('RegTech'), the barriers to the uptake of these technologies and the regulatory and other initiatives necessary to promote these technologies in Australia: see *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 1.

Committee on Australia as a Technology and Financial Centre'),[107] and the Inquiry into Future Directions for the Consumer Data Right,[108] were in agreement that, for the time being, maintaining the status quo was preferable to taking regulatory action.[109] In response to the proposal by the Reserve Bank of Australia ('RBA') to examine whether a ban on SS would support the financial sector's transition away from the practice, the Inquiry admitted, however, that for *payment initiation services* the eventual prohibition of SS would be in the interests of consumers.[110] Indeed, without proper safeguards, 'payment initiation', aka 'action initiation' or 'write access', could enable a third party to act in ways contrary to the consumer's express instructions, causing her substantial harm.[111] Yet, in contrast to the EU and the UK frameworks, which specifically regulate payment initiation, CDR is currently limited to 'read access', meaning that, while consumers are able to share data with third parties, they cannot instruct them to take actions on their behalf. This, too, was the drafters' conscious decision: action initiation was viewed as premature and likely to endanger the framework's acceptance.[112] The Australian government was particularly mindful that, for CDR to succeed, consumers must first gain confidence in their data being accessed and shared securely and only for the purposes to which they have consented.

In response to the Inquiry the government announced, in December 2021, that it would 'expand the functionality of the CDR regime to include support for consumer-directed third-party action initiation' in the banking sector.[113] Indeed, the bill proposing to extend the CDR framework to introduce action initiation was finally introduced into Parliament in November 2022 and, in May 2023, the Senate Economics Legislation Committee presented its report on the bill and recommended that it be passed.[114] At the time of writing it is hard to tell, however, when the use of action initiation will become widespread. In the Inquiry's view, a

---

107 'Select Committee on Australia as a Technology and Financial Centre', *Parliament of Australia* (Web Page, 18 March 2021) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology>.

108 The inquiry was tasked to make recommendations on how to expand the CDR's functionality in a manner that promotes innovation with the consumer interests in mind: see The Australian Government the Treasury, *Inquiry into Future Directions for the Consumer Data Right* (Report, Treasury, October 2020) viii ('*Inquiry into Future Directions*').

109 See *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 220 (Recommendation 22). See also *Inquiry into Future Directions* (n 108) 36, 96–7.

110 *Inquiry into Future Directions* (n 108) 97 (emphasis added).

111 'Read access is the ability for a third party to download or view specific information held by the data holder, while write access is the ability for the third party to give the data holder instructions to take actions': ibid 18, 20.

112 *Review into Open Banking* (n 1) 109.

113 This will enable third party 'payment initiation' as well as 'general action initiation', including switching between products and services, opening or closing an account, updating details, etc: see Australian Government, 'Government Response to the Final Report of the Inquiry into Future Directions for the Consumer Data Right' (Response, 14 December 2021) 2 <https://treasury.gov.au/publication/p2021-225462>.

114 *Treasury Laws Amendment (Consumer Data Right) Bill 2022*; Consumer Data Right, 'Consumer Data Right Newsletter' (26 May 2023) *Consumer Data Right Updates*.

ban on SS will only be timely once payment initiation achieves 'a broad coverage' of banks and accounts.[115]

The Labor government that came to power in Australia in May 2022 asserted its full support for the CDR regime.[116] However, the volume of data being shared via Open Banking has not been made public in Australia, making it hard to assess the extent to which SS remains a serious contender to APIs in the context of financial data access and sharing.[117] The ACCC guidance for the industry from March 2021 notes only that businesses collecting data via both channels must be transparent with consumers as to how the data is collected and which protections apply.[118] Given that Australia has not yet formally phased out SS, it is safe to assume it remains a popular practice.[119]

IV SS – To Use or Not to Use?

Although the range of services enabled by SS have evolved and diversified significantly since the end of the 1990s, many of the arguments for and against SS are not new. Incumbent institutions (banks) and new entrants (FinTechs) often find themselves at opposite ends of the arguments. Perhaps unsurprisingly, almost every single argument has been met with a counterargument.

A *The Downsides of SS ('Long Live APIs!')*

The arguments against SS are many. The foremost is that handing over user credentials is an inherently unsafe online behaviour, which runs counter to good IT security practices and the explicit security advice provided by governments and most businesses to consumers.[120] Where the third party possesses user credentials, it has nearly unlimited control over the customer's account: it can

---

115 *Inquiry into Future Directions* (n 108) 97.

116 See Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, 'Happy First Birthday, CDR!', *Consumer Data Right Newsletter* (1 July 2022). See also James Eyers, 'Open Banking Still Has Teething Problems after Two Years', *Australian Financial Review* (online, 5 July 2022) <https://www.afr.com/companies/financial-services/open-banking-still-has-teething-problems-after-two-years-20220704-p5ayt0>.

117 Eyers (n 116).

118 See ACCC Team OLD, 'Guidance on Screen-Scraping', *Consumer Data Right* (Web Page, 23 March 2021) <https://cdr-support.zendesk.com/hc/en-us/articles/900005316646-Guidance-on-screen-scraping>; Joseph Brookes, 'ACCC Warning on "Screen Scraping" and CDR Data', *InnovationAus.com* (online, 23 March 2021) <https://www.innovationaus.com/accc-warning-on-screen-scraping-and-cdr-data/>.

119 'The consultation process revealed that there is still significant use of screen scraping in sectors both within and outside the CDR': The Australian Government the Treasury, *Statutory Review of the Consumer Data Right* (Report, September 2022) 28 ('*Statutory Review of the Consumer Data Right*'). See also TrueLayer (n 86) 10.

120 Evidence to Select Committee on Financial Technology and Regulatory Technology, Senate, Parliament of Australia, Melbourne, 30 January 2020, 33 (Xavier Shay); Evidence to Select Committee on Financial Technology and Regulatory Technology, Senate, Parliament of Australia, Melbourne, 30 January 2020, 13 (Lisa Schutz).

access data it has not been authorised to access, execute financial transactions without the permission of the customer, and even change the customer's authentication credentials thereby locking them out of their own accounts.[121] Moreover, extending user credentials to a third party inevitably creates a larger surface area for cyberattacks, including phishing attacks and unwanted profiling.[122] As a rule, businesses relying on SS will need to submit the customer credentials in unencrypted form to the server from which the data is to be scraped.[123] As a result, risks of fraud and unauthorised access to customers' accounts are compounded, as their login credentials are exposed in multiple places.

A further argument against SS is that the security and reliability of FinTechs does not compare with the security and reliability of the financial institutions hosting the accounts and issuing the user credentials.[124] In Australia, for example, CBA has argued that customers who have used the services of FinTechs relying on SS are at least twice as likely to experience digital fraud, compared to customers who do not share their account credentials.[125] Even though CBA could not prove that customer losses were caused by sharing personalised user credentials with third parties, it identified a 'very concerning correlation', which suggested that customers who had logged onto their online accounts via intermediaries were more likely to experience fraud.[126]

Giving third parties access details to one's bank account also amounts to a breach of the banks' customer terms and conditions and — in Australia — places customers at risk of losing their protections under the E-Payments Code. The E-Payments Code administered by ASIC applies to consumer electronic payment transactions as set out in cl 2.5 of the Code (including electronic card transactions, telephone banking, certain online transactions and online bill payments, direct debits and others).[127] Although a voluntary code of practice, it is adhered to by most banks, credit unions and building societies along with a number of non-banking businesses.[128] Under the E-Payments Code, consumers must not voluntarily disclose passcodes to anyone, including a family member or friend, and if they do so, they may be liable for damages that occur as a result of handing

---

121 Bank for International Settlements, *Report on Open Banking and Application Programming Interfaces* (Report, November 2019) 9.

122 Amanda Cliffe, 'To What Extent Does European Law Ensure a Level Playing Field for Fintechs in the Payment Services Sector?' (2022) 18(1) *European Competition Journal* 168, 174.

123 GoCardless, 'Screen Scraping 101: Who, What, Where, When?', *The Open Banking Hub* (Web Page, 19 July 2017) <https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712>.

124 Jane Winn and Benjamin Wright, *The Law of Electronic Commerce* (Wolters Kluwer, 4th ed, 2021) 7–130.

125 James Eyers, 'CBA Says Using Fintechs Exposes Customers to Account Fraud', *The Australian Financial Review* (online, 16 March 2020) <https://www.afr.com/companies/financial-services/cba-says-using-fintechs-exposes-customers-to-account-fraud-20200316-p54amd>.

126 Ibid.

127 Australian Securities and Investments Commission, *ePayments Code* (2 June 2022).

128 Ibid.

over their credentials.[129] While a breach of the passcode security requirements in itself is insufficient to impose liability for losses from an unauthorised transaction on a consumer, a consumer is liable where a service provider can prove on the balance of probability that they contributed to a loss through fraud, or breaching the pass code security requirements.[130]

One problem, however, is that consumers may not even realise they lose protection under the E-Payments Code. As noted by the Review into Open Banking in Australia, in some instances 'the way in which a request for a customer's bank login details is made means that customers may not even be aware they have given their login details to someone other than their bank.'[131] Alternatively, a consumer may naively presume the legality of credential sharing. She may think that, because a FinTech engaged in SS collects data from her financial institution, there would be a legal relationship between the two entities that requires or validates the consumer's cooperation.[132] Either way, the consumer is being exploited to an extent unfathomable under data-sharing arrangements via APIs, which ensure transparency in the way consumers are able to grant and revoke access to their data and which ensure consumers know how, when and for what purposes their data is used.[133]

There is broad agreement in the industry that SS has historically been relied upon out of necessity rather than because it is an elegant technology design for data sharing.[134] SS is largely regarded as a slow and unstable method of data collection, which is frequently prone to errors. Specifically, SS methods are based on navigating whole web pages, requiring a lot of data to be downloaded and processed to get a few sought-after pieces of information. They are thus much slower than APIs, which establish a direct connection between a data holder and a data recipient.[135] In fact, assessments claim that processes that take SS tools up to ten minutes can be completed in seconds by using dedicated interfaces.[136] Further, SS is a workaround rather than a dedicated solution. It requires maintaining a unique script for each dedicated data source (ie for each individual bank). Should the bank's platform change ever so slightly (for example, a button on the online user interface is moved from one part of the page to another), SS

---

129 See *ePayments Code* (n 127) cls 11.1–11.2, 12(2)(a). See also *Review into Open Banking* (n 1) 72, which notes '[h]anding over login credentials to enable screen scraping may be a violation of the bank's terms and conditions, meaning the customer may be liable if their credentials were to be compromised.'

130 *ePayments Code* (n 127) cl 11.2.

131 *Review into Open Banking* (n 1) 52.

132 *Account Aggregation* (n 3) 26.

133 Adatree (n 40).

134 *Review into Open Banking* (n 1) 72.

135 See Tonia Berglund, 'From Screen Scraping to Open Banking', *Australian Broker* (Web Page, 1 July 2021) <https://www.brokernews.com.au/features/opinion/from-screen-scraping-to-open-banking-277582.aspx>.

136 Kelly Read-Parish, 'Open Banking vs Screen Scraping: Looking Ahead in 2019', *Finextra* (Web Page, 4 January 2019) <https://www.finextra.com/blogposting/16494/open-banking-vs-screen-scraping-looking-ahead-in-2019>.

won't work, thereby necessitating a re-write of the script by the developer to re-establish the connection.[137] The need to repeatedly fix connectivity issues resulting from web updates means that the end-user is likely to experience unstable performance.[138] Lastly, SS runs on image processing, and is therefore argued to be prone to errors.[139]

Understandably, incumbents oppose SS because of their inability to control how much data (including 'collateral data'), and how often data, is scraped. SS places enormous demands on the IT infrastructure of financial institutions, increasing costs and operational risk. In the US, for example, data aggregators like Plaid and Mint have been found to make up to 20 per cent of a typical bank's traffic and typically log in 2.5 times as often as real users.[140] Some sources suggest that data aggregators may even represent up to 25 per cent of financial institutions' total traffic.[141] This problem of burdening the servers of the data host does not arise with APIs.

Opponents of SS also argue that allowing the practice to continue undermines the potential success of Open Banking by creating a two-tiered system where less trustworthy operators are likely to prefer using SS.[142] Indeed, Open Banking regimes impose stringent cybersecurity and privacy protection requirements, which businesses using SS can circumvent.[143] As aptly pointed to by the ACCC, this means that businesses using unregulated data-sharing methods such as SS 'have a lower regulatory burden than those whose businesses involve CDR data.'[144] Indeed, to secure optimum data safety for consumers, primarily accredited entities are allowed to share customer data via Open Banking.[145] However, why would a FinTech want to undergo a time-consuming and costly process of accreditation and be subject to stringent data access, handling and

---

137 Cardinal and Thomas (n 14) 94; Vitor Urbano, '5 Reasons Why You Should Say NO to Screen Scraping', *Nordigen* (Web Page, 6 October 2021) <https://nordigen.com/en/blog/5-reasons-why-you-should-say-no-screen-scraping-when-using-open-banking/>; *Review into Open Banking* (n 1) 72.

138 Roland Mesters, 'Can We Please Stop Using Screen Scraping for Bank Connectivity?', *Finextra* (Web Page, 14 December 2021) <https://www.finextra.com/blogposting/21403/can-we-please-stop-using-screen-scraping-for-bank-connectivity>. See also MX Technologies, 'Screen Scraping Vs. Bank APIs: What's the Difference?', *MX Blog* (Web Page, 4 August 2020) <https://www.mx.com/blog/screen-scraping-vs-bank-apis-whats-the-difference/>.

139 Deepa Bhat, 'Screen Scraping vs API: 10 Questions to Understand the Differences', *Medium* (Web Page, 12 October 2018) <https://medium.com/yapily/screen-scraping-vs-api-10-questions-to-understand-the-differences-dc63fe19e3ed>.

140 F5, 'Easiest Way to Manage Financial Aggregators', *Video* (Web Page, 27 October 2022) <https://www.f5.com/solutions/financial-aggregators>.

141 Olov Renberg, 'Fintech Aggregators and Open Banking: Service Enablers or an Unfortunate Backdoor for Fraud?', *BehavioSec* (Blog Post, 8 December 2021) <https://www.behaviosec.com/blog/fintech-aggregators-and-open-banking-service-enablers-or-an-unfortunate-backdoor-for-fraud/>.

142 Financial Rights Legal Centre and the Consumer Action Law Centre (n 37) 16. See also TrueLayer (n 83) 11.

143 TrueLayer (n 86) 10.

144 Australian Competition and Consumer Commission, Submission to the Treasury, *Statutory Review of the Consumer Data Right* (May 2022) 3 <https://treasury.gov.au/sites/default/files/2022-09/c2022-314513-australian_competition_and_consumer_commission.pdf>.

145 See *CCA* ss 56BB(d), 56BH; *CDR Rules* (n 99) rr 1.9, 5.12; *PSR* (n 69) pts 2, 3.

transfer obligations, if data can be freely accessed via SS? Opponents of SS therefore warn of its capacity to split the FinTech sector into businesses which adhere to higher standards and security requirements and those that do not.[146]

Last but not least, it is argued that investing in SS is a waste of financial resources because SS will become a defunct technology.[147]

B *The Advantages of SS ('Long Live SS!)*

Proponents of SS, however, insist that the technology should be retained. SS has long been regarded as an effective tool to address significant information asymmetry in finance and drive competition.[148] Historically, incumbent players — banks — treated customer data as their own by capturing and siloing it on their servers.[149] This created substantial barriers for new market entrants who needed the data to successfully shape their product and services portfolios and drive their businesses. SS has helped to remove those barriers, behind which the banks were sheltering, and enable FinTechs to better compete.[150] In turn, incumbents have been pushed to improve their own service offerings. As a result, some view SS as the single most important driver of use-case development globally.[151]

As data transfer technology, SS has been favoured by businesses for a range of reasons, the foremost being business convenience and efficiency at a relatively low cost. A FinTech with a customer's account credentials does not need to enter into contractual arrangements with the account-holding institution to access customer data.[152] Without account credentials, a FinTech needs to negotiate data access via structured data feeds – ie APIs – which is time-consuming and costly. Where API connections are not available, the service to the customer cannot be provided at all and the customer is lost. Even where APIs are 'open' — that is, characterised by their free or low-cost availability to third parties and a relatively standardised format[153] — building connections to APIs, testing and maintaining

---

146 Financial Rights Legal Centre and the Consumer Action Law Centre (n 40) 17.

147 Ibid 18.

148 Illion, Submission to the Treasury, Parliament of Australia, *Inquiry into Future Directions for the Consumer Data Right* (11 May 2020) 4.

149 Note that as a matter of law, no property rights in data exist, merely the right to control it. See, eg, Heiko Richter, 'The Power Paradigm in Private Law' in Mok Bakhoum et al (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Regulation of Personal Data* (Springer, 2018) 527, 553. See also Thomas Tombal, *Imposing Data Sharing Among Private Actors: A Tale of Evolving Balances* (Wolters Kluwer, 2022) [63]. See also World Bank, 'Ownership: Who owns personal data?' *World Development Report* (Web Page, 2021) <https://wdr2021.worldbank.org/spotlights/who-owns-personal-data/>.

150 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 145 [5.57].

151 Arab Regional Fintech Working Group, 'Open Banking Regulatory Principles' (Report No 164, Arab Monetary Fund, March 2021) 13.

152 Cliffe (n 122) 174.

153 Cardinal and Thomas (n 14) 93.

those connections requires investment of money and time.[154] Indeed, some argue that building API connections is more difficult than developing APIs, particularly where the goal is to connect with multiple financial institutions in multiple markets.[155]

To illustrate, there are currently three main API standards in Europe — STET PSD2 API framework, UK Open Banking Standard, and Berlin Group's NextGenPSD2 XS2A Framework Standard — each with different specifications or requirements for its region which then are often further particularised by individual banks.[156] Whereas each ASPSP has, at most, one API to implement, AISPs and PISPs must implement a large number of APIs, depending on their current services and market coverage.[157] Monitoring the API connections for downtime, upgrades, and improvements also results in significant and ongoing work which compels many businesses to outsource these tasks to external providers.

Accreditation requirements may also incentivise recourse to SS. In Australia, for example, the time and money that needs to be invested to obtain accreditation under the CDR (and thus be able to share customer data via standardised APIs) are argued to be barriers too steep for many FinTechs to overcome. Smaller companies and start-ups thus often prefer to rely on SS.[158]

In contrast, the technical set up for receiving data via SS is said to be fast, as it bypasses the data holder's systems and data-sharing permissions.[159] Most importantly, SS is argued to offer access to both larger volumes of, and more granular, data.[160] This data can be stored digitally in a data collector's database (be it a service providing FinTech or a data aggregator acting as an intermediary) and accessed without restriction for as long as customer credentials do not change or permission for data access is not revoked.[161] In comparison, connecting via dedicated interfaces may well be less attractive, as banks may not only limit the data that is accessible through APIs, but also reduce the connection speed or API's availability.[162]

---

154 Tink AB, 'Why Connecting to Open Banking APIs Is Not as Simple as It Seems', *Tink* (Web Page, 19 August 2021) <https://tink.com/blog/open-banking/complexities-behind-open-banking-connections/> ('Connecting to Open Banking APIs'); Ayers and Bhattacharyya (n 39).

155 Tink AB (n 154).

156 Ibid. See also Andrei Cazacu, 'PSD2: Does Europe Need a Single API Standard?', *TrueLayer* (Blog Post, 13 July 2022) <https://truelayer.com/blog/psd2-does-europe-need-a-single-api/>.

157 World Bank, 'Technical Note on Open Banking: Comparative Study on Regulatory Approaches' (Technical Note, 2022) 21. See also Inna Oliinyk and William Echikson, 'Europe's Payments Revolution: Stimulating Payments Innovation while Protecting Consumer Privacy' (Research Report No 2018/06, Centre for European Policy Studies, September 2018) 3.

158 Berglund (n 135). See also Natalia Jevglevskaja and Ross P Buckley, 'The Consumer Data Right: How to Realise This World-Leading Reform' (2022) 45(4) *University of New South Wales Law Journal* 1589 ('The Consumer Data Right').

159 Adatree (n 40).

160 *PSD2* (n 43); Wandhöfer (n 63) 192–3 [12.020].

161 Financial Data Exchange (n 37) 5.

162 Wolters and Jacobs (n 63) 35.

Business advantages, however, are not the sole grounds that SS proponents use to defend it. Alleged consumer benefits are brought into the debate too. When employed by responsible actors that have safeguards in place to duly protect consumer data, SS has been argued to be a viable technology that is 'valued by consumers'.[163] It also helps them realise their autonomy, since consumers have a right to decide whether they want their data to be shared via SS or via alternative techniques.[164] Some businesses argue that, if consumers are given a choice between using a quicker digital assessment processes based on SS and a manual paper-based assessment, which takes considerably longer, over 80 per cent of consumers choose the faster, digital option.[165]

Finally, the retention of SS practices has been defended on the grounds that they offer a benchmark against which to judge the success of Open Banking. In Australia, for example, the Review into Open Banking emphasised that allowing competing approaches would provide an important test of the design quality of Open Banking: 'Should those competing approaches become more actively used than those specified under Open Banking, this will provide a valuable signal to regulatory authorities that the design of Open Banking may need to be revisited.'[166] Besides, some project that there will be a broad range of complementary use cases for SS even when Open Banking has been fully implemented.[167] For example, SS may be needed to supplement API-derived data, where the level and quality of the latter proves insufficient or poor (for instance, SS may be used to help clean and correct Open Banking data parcels and perform data reconciliation[168]), or to provide a redundancy fail-safe in an event that the APIs of the financial institution hosting the customer account are offline or do not function properly.[169]

V SS – To Ban (Full Stop)

As Australia continues its march towards an economy in which an increasing volume of consumer data is shared, the hybrid model where data can be derived

---

163 Illion (n 148).

164 Ralf Ohlhausen, 'Why the EBA Is Wrong about Screen Scraping, and How It Will Hurt European Fintech', *inFinite Intelligence* (Web Page, 3 April 2017) <https://www.bobsguide.com/articles/why-the-eba-is-wrong-about-screen-scraping-and-how-it-will-hurt-european-fintech/>.

165 Illion, Response to a Question on Notice to Senate Select Committee on Financial Technology and Regulatory Technology, *Inquiry into the Current State of Australia's FinTech and RegTech Industries* (17 February 2020) 2. See also *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 146 [5.63].

166 *Review into Open Banking* (n 1) 10. See also Illion (n 148) 4.

167 Berglund (n 135).

168 FinTech Australia, Submission No 19 to Senate Select Committee on Financial Technology and Regulatory Technology, *Australia as a Technology and Financial Centre* (September 2019) 35.

169 Illion (n 148) 5.

from both SS and dedicated interfaces appeals to many businesses.[170] In their opinion, it is critically important that SS continues to be available to consumers and their service providers into the foreseeable future.[171]

To those who disagree, they respond that today's business models typically limit the number of parties that need to hold customer credentials to renowned aggregation firms (such as MX, Finicity, Envestnet | Yodlee, Plaid, and others) that provide their services to a large number of FinTechs and (allegedly) use encryption and bank standard security measures to keep customer data safe.[172] Some even suggest that SS technology has evolved so considerably that, from a security standpoint, little difference exists between SS and data access via APIs.[173] Crucially, these businesses contend that no significant evidence of consumer detriment or security breaches occurring because of SS can be demonstrated to date.[174]

Admittedly, when questioned about SS at a public hearing of the Senate Select Committee on Financial Technology and Regulatory Technology, ASIC Commissioner Sean Hughes confirmed that ASIC was not aware of any evidence of consumer loss occurring from SS.[175] It is equally worth noting that reliance on APIs is not always risk free. An Akamai report has found that, from May to October 2019, credential stuffing[176] attacks on the financial services industry targeted APIs, often accounting for 75 per cent or more of the total login attacks against financial services.[177] Breaches frequently occur where API authentication is poorly implemented, allowing attackers to assume legitimate users' identities.[178]

---

170 See, eg, ibid 5. Finder, Submission to the Treasury, *Statutory Review of the Consumer Data Right* (May 2022) 10.

171 Illion (n 148) 5. Finder (n 170).

172 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 145 [5.57], 146 [5.60]. See also *Review into Open Banking* (n 1) 73. See also United States Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech and Innovation* (Report, 2018) 37, 87. On the impact of big data aggregation businesses on the future of data sharing generally, see Dan Awrey and Joshua Macey, 'The Promise & Perils of Open Finance' (2023) 40(1) *Yale Journal on Regulation* 1, et seq.

173 See, eg, arguments offered by Illion and RAIZ Invest Limited to the *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 145–6 [5.57]–[5.61]. See also Kathy Shi, 'ASIC & ACCC: Screen Scraping Is a Valid Method of Data Sharing', *Basiq* (Blog Post, 9 March 2020) <https://basiq.io/blog/asic_accc_screen_scraping_is_a_valid_method_of_data-sharing/>.

174 See, eg, statement by RAIZ Invest Limited: '[s]creen scraping has existed in Australia for over 5 years. It is widely used by many companies, including ANZ and Xero with no reported security or fraud issues in those 5 years': RAIZ Invest Limited, Submission No 29 to Senate Select Committee on Financial Technology and Regulatory Technology, *Australia as a Technology and Financial Centre* (September 2019) 4.

175 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 146 [5.62].

176 Credential stuffing is a type of cyberattack in which attackers use lists of compromised user credentials to obtain access to a system: see Imperva, 'What Is Credential Stuffing', *Imperva* (Web Page, 2023) <https://www.imperva.com/learn/application-security/credential-stuffing/>.

177 Akamai, 'Financial Services: Hostile Takeover Attempts' (Report Volume 6, *State of the Internet / Security Reports*, February 2020) 2.

178 Accenture, 'Catching the Open Banking Wave' (Report, *Accenture*, 2021) 14.

With data quality under CDR being another issue calling for improvement, FinTechs have yet another card to play in defence of SS.[179] The Financial Data and Technology Association ('FDATA') notes, for example, that many of its members frequently complain about poor quality data and delays in receiving data.[180] Yet the argument that the security of data transfers by SS equals that of transfers by dedicated interfaces fails to persuade. There may not yet have been significant consumer losses from SS, but this does not mean they are improbable. Personalised security credentials, if shared with perceived benevolent actors, can be readily compromised by malicious third parties and exploited to the detriment of the customer. The greater the amount of consumer financial account and transaction data collected and retained by data aggregators, the greater the potential damage to consumers from a data breach.[181] Where businesses employing SS technology offer 'action initiation' as opposed to merely 'read access' solutions, the harm to consumers is likely to be even greater.[182]

A *SS Facilitates Predatory Lending*

Most importantly, the advantages of SS sit largely with the business community, not consumers, who are left vulnerable to having their data exploited in ways of which they are unaware. The argument that SS exists because of 'consumer demand' and 'consumer convenience' as a hassle-free way of obtaining financial services, such as small loans, is unsustainable. Faced with a choice between manually collecting, organising and presenting the required financial data in a format preferred by the lender, or letting the latter obtain and collate the data, some consumers will hand over their banking credentials, and some will not. Yet when consumers are excluded from accessing mainstream credit lines and the only available providers use SS, no true choice exists for consumers between obtaining credit and keeping their credentials safe.[183] Such a scenario does not demonstrate conscious consumer 'demand' or choice. It is unlikely that many Australian consumers would choose SS were they also given the option of sharing their data via more secure dedicated interfaces as under Open Banking.

In the light of the general expectation that Open Banking will make the practice of SS obsolete in due course, one may question the value of an explicit ban on this method of data collection. However, CDR's full implementation in banking and finance, which commenced in July 2020,[184] will seemingly take many more

---

179 *Statutory Review of the Consumer Data Right* (n 119) 31, 7 (finding 2.1).

180 Financial Data and Technology Association, Submission to the Treasury, *Statutory Review of the Consumer Data Right* (April 2022) 17; Finder (n 170) 6.

181 United States Department of the Treasury (n 172) 37.

182 *Review into Open Banking* (n 1) 108.

183 Financial Rights Legal Centre and the Consumer Action Law Centre (n 40) 17.

184 Phase 1 of the CDR implementation in open banking: see Australian Competition and Consumer Commission, 'Consumer Data Right' (Phasing, December 2020) <https://www.cdr.gov.au/sites/default/files/2021-01/CDR%20phasing%20table%20-%20January%202021.pdf>.

years. The process is slow, and it is consumers who bear the brunt of the potential adverse effects of SS in the meantime. Unlike other jurisdictions, Australia's FinTech industry is heavily reliant on SS.[185] One of its most concerning uses is in the lending sector, where the practice is prevalent throughout the small loans market, such as payday lending.[186]

The demand for such small loans from providers other than major banks and credit societies expanded rapidly in the late 1990s, as data aggregation by SS began to proliferate, and the provision of such loans by banks and credit societies began to decline.[187] Personal circumstances, such as adverse credit history or unemployment, restrict the ability of many Australians to access mainstream credit products. In the case of payday loans, however, these restrictions generally do not apply. Most payday loans are 'small amount credit contracts' under the *National Consumer Credit Protection Act 2009* (Cth), that is loans to consumers of up to $2,000 where the credit provider is not an authorised deposit-taking institution ('ADI') and the contract term is between 16 days and 12 months.[188] Payday loans are characterised as a form of emergency finance.[189] The *Caught Short Interim Report*, for example, found that poverty pervades the lives of most borrowers of payday loans who 'live in such impoverished circumstances that notions of customer choice lose meaning'.[190]

Data shows that, between April 2016 and July 2019, over 4.7 million individual payday loans were taken out by around 1.77 million households worth approximately AUD $3.09 billion.[191] This constitutes a not insignificant share of the global payday loan market, which in 2021 was valued at USD $33.5 billion, and is projected to reach USD $42.6 billion by 2028.[192] While there are caps on fees that loan providers may charge, such as a one-off establishment fee of not more than 20 per cent of the loan amount and a monthly account keeping fee of not more than 4 per cent of the loan amount,[193] the monthly fee does not reduce over time

---

185 FinTech Australia, Submission to the Treasury, *Review into Open Banking in Australia* (September 2017) 5.

186 Financial Rights Legal Centre and the Consumer Action Law Centre (n 40) 10.

187 Paul Ali, Cosima McCrae and Ian Ramsay, 'The Politics of Payday Lending Regulation in Australia' (2013) 39(2) *Monash University Law Review* 411, 418.

188 See *National Consumer Credit Protection Act 2009* pts 1–2.

189 Senate Economics References Committee, *Credit and Hardship: Report of the Senate Inquiry into Credit and Financial Products Targeted at Australians at Risk of Financial Hardship* (Report, 22 February 2019) 2. See also Marcus Banks et al, *Caught Short: Exploring the Role of Small, Short-Term Loans in the Lives of Australians* (Final Report, August 2012) 32.

190 Marcus Banks, *Caught Short: Exploring the Role of Small, Short-Term Loans in the Lives of Australians* (Interim Report, September 2011) 8, 23 ('*Caught Short Interim Report*').

191 Consumer Action Law Centre, *The Debt Trap: How Payday Lending Is Costing Australians* (Report, November 2019) 4.

192 Vantage Market Research, '2022 Statistics: Payday Loans Market Will Surpass USD 42.6 Billion at 4.1% CAGR Growth', *GlobeNewswire* (Web Page, 3 May 2022) <https://www.globenewswire.com/en/news-release/2022/05/03/2434258/0/en/2022-Statistics-Payday-Loans-Market-Will-Surpass-USD-42-6-Billion-at-4-1-CAGR-Growth-Vantage-Market-Research.html>.

193 Australian Securities and Investments Commission 'Loans and Credit Cards', *Australian Securities and Investments Commission* (Web Page, 27 October 2022) <https://asic.gov.au/for-consumers/loans-and-credit-cards/>.

as the loan is repaid but applies every month to the original amount borrowed. As a result, depending on the loan duration, the equivalent interest rate is often around 100 per cent per annum, and at times very much higher.[194]

With payday loans increasingly obtained online,[195] consumer-rights organisations warn that:

> some nonbank lenders obtain consumer's bank account passwords to screen scrape financial data. In so doing they hold on to these passwords and use them at later times to identify if a bank account is low in funds. If the account *is* low in funds they then proceed to spam the consumer with direct marketing material offering further high cost loans. While access to quick credit may lead to benefits for some consumers, the reality is that this unscrupulous behaviour pushes many people into a spiral of debt.'[196]

The asymmetry of power and information between a financially vulnerable consumer and a payday lender with access to their financial information is considerable. Even if the lender is not exploitative or fraudulent, the customer may be ill-informed, unsuspecting, or unable to properly evaluate the loan offer.[197] Certainly, payday lending addresses the financial needs of *some* consumers who are able to pay off the loan on time. But this industry is not built upon these responsible, savvy consumers. It is built upon the ignorant and the vulnerable, who become over-indebted and trapped, and upon the stream of late fees and other charges their credit contracts impose upon them. Overall, the practice is deeply exploitative and harms far more Australians than it assists. While banning SS is not going to prevent payday lending, it will, at the least, make it harder to prey on consumers low in cash. When predatory lenders no longer have access to information as to the state of a customer's account, they will need to compete on equal terms with other lenders under the CDR. Lenders with less 'aggressive' loan conditions will hopefully win customers thereby potentially bringing down fees and interest rates on payday loans in the long term.

B *SS Slows the Rollout of the CDR*

Another reason for regulatory intervention on SS is the problem of industry inertia which, if not addressed, may slow the implementation and acceptance of the CDR. Joining the regime involves meeting stringent regulatory requirements to ensure that consumers develop trust and confidence in the system. Without an outright ban, organisations who may consider data sharing via CDR as 'too hard',

---

194 Consumer Action Law Centre (n 191) 6.

195 While only 5.6 per cent of payday loans originated online in 2009, the figure was expected to hit 85.8 per cent in 2019: see Consumer Action Law Centre (n 191) 4.

196 Financial Rights Legal Centre, Financial Counselling Australia, and Consumer Actions Law Centre, Submission to the Treasury, *Consumer Data Right: Sectoral Assessment for Non-Bank Lending* (14 April 2022) 5. See also Consumer Action Law Centre (n 191) 4, which notes that 'over a five-year period, around 15% of payday loan borrowers fall into a debt spiral.'

197 Financial Rights Legal Centre and the Consumer Action Law Centre (n 40) 12.

such as payday lenders or debt management firms, will continue relying on SS without regard for the consumer.[198] The facts on the ground appear to prove this assumption. In 2017, FinTech Australia found that many FinTech companies were 'happy with existing screen scraping solutions, and [were] likely to continue to use these solutions even when alternative technology was available'.[199] In 2020, the Senate Select Committee on Financial Technology and Regulatory Technology confirmed that the technology was *widely used* by banks, lenders, financial management applications, personal finance dashboards, and accounting products.'[200] As of 2021, only 7 per cent of FinTechs in Australia had become Accredited Data Recipients ('ADRs').[201] A further 25 per cent intended to follow suit, while others were planning on participating in the CDR regime via an intermediary.[202]

While some service providers are starting to replace collecting customer data by SS with accessing information through the CDR,[203] the numbers remain conspicuously low. Only a handful of FinTechs in Australia are ready and willing to turn their back on SS for most use cases. Frollo, for example, recently announced that it has phased out SS for the major big four banks in Australia — Australia and New Zealand Banking Group ('ANZ'), Commonwealth Bank ('CBA'), National Australia Bank ('NAB'), and Westpac.[204] Generally thought of as the best money-management app,[205] and one of the first FinTech companies accredited under CDR, it added that it would progressively phase out screen scraping for other banks 'until it's only used for banks and products not covered under the CDR'.[206]

---

198 Liu (n 41) 327. See also Jill Berry, 'If the Australian Government Truly Cares about Privacy, then It's Time to Ban Screen Scraping', *Startup Daily* (Web Page, 7 March 2022) <https://www.startupdaily.net/topic/data/if-the-australian-government-truly-cares-about-privacy-then-its-time-to-ban-screen-scraping/>.

199 FinTech Australia, Submission to the Treasury, *Review into Open Banking in Australia* (September 2017) 8.

200 *Senate Select Committee Interim Report on Financial Technology and Regulatory Technology* (n 9) 143 [5.50].

201 May Lam and Malia Forner, 'Australian Fintech Sector Creating Jobs and Raising Capital, with Sights Set on Overseas Markets', *EY* (Web Page, 20 October 2021) <https://www.ey.com/en_au/economics/australian-fintech-sector-creating-jobs-and-raising-capital>.

202 Ibid. The inaugural version of the CDR Rules set out one general level of accreditation – the 'unrestricted' level – which provides access to all CDR data within scope for banking. On 30 September 2021, the rules were amended to introduce the sponsored level of accreditation, which permits a person to seek accreditation at a new 'sponsored' level if they have arrangements with an accredited person with an unrestricted level of accreditation (a 'sponsor'): see generally Australian Government, 'Accreditation Guidelines: Version 3' (Guidelines, February 2022) <https://www.cdr.gov.au/sites/default/files/2022-02/CDR-Accreditation-guidelines-version-3-published-16-February-2022.pdf>.

203 Productivity Commission, '5-Year Productivity Inquiry: Australia's Data and Digital Dividend' (Inquiry Interim Report No 2, 23 August 2022) 46.

204 Frollo, 'Frollo Phases out Screen Scraping in Favour of Open Banking', *Frollo* (Blog Post, 9 August 2022) <https://frollo.com.au/blog/phasing-out-screen-scraping/>.

205 Ava Crawford, 'Meet Frollo: Australia's Best Money Management App of 2022', *Mozo* (Web Page, 17 March 2022) <https://mozo.com.au/neobanks/articles/meet-frollo-australia-s-best-money-management-app-for-2022>.

206 Frollo (n 50) (emphasis added).

That SS can be regulated is demonstrated by the approaches to this practice taken in the EU and UK discussed above. Their limitation to payment accounts notwithstanding, the EU and UK frameworks serve as a precedent from which the Australian government can draw both insight and inspiration. As explained previously, where an account-holding institution is exempt from providing a contingency mechanism, AISPs and PISPs are barred from using SS technology in relation to customer payment accounts (ie both with or without identification towards the ASPSPs). While exact numbers are hard to find, some sources suggest that many banks indeed benefitted from the said exemption suggesting that the impact of *PSD2* on SS may be larger than expected.[207] In the UK in particular, the number of API calls surged significantly: from 12 million a day in February 2020 to 24 million a day a year later, and up to 31 million a day in February 2022, or 860 million calls for the month.[208] The UK experience in particular shows that even partial phasing out of SS can act as a spur to ensure that APIs perform well and the ecosystem grows rapidly and with due attention to data quality.[209]

As noted previously, the Inquiry into Future Directions for the Consumer Data Right observed that the prohibition on SS would be desirable once action initiation under CDR is fully implemented as a viable alternative. Likewise, the *Statutory Review of the Consumer Data Right* recommended that SS be banned in sectors where the CDR is functioning as intended.[210] Commendably, the Australian Government has most recently indicated that it will consult on policy options for regulating SS, commencing in the banking sector and starting with the release of a discussion paper in the second half of 2023.[211] For the reasons presented in this article, and given the government's commitment to the success of the CDR, assessment of, and the decision on how best to, address the problem of SS in Australia should not be postponed for too long. Importantly, an advance indication from government on how and when a ban is likely to be implemented would offer certainty and time for businesses to move away from SS and provide stronger incentives to invest in transitioning to the CDR.[212]

---

207 Tink AB, 'What the EBA Putting Its Foot Down on PSD2 API Obstacles Really Means', *Tink blog* (Blog Post, 2 March 2021) <https://tink.com/blog/open-banking/eba-opinion-psd2-api-obstacles-fallback-exemptions/>. See also European Banking Authority, 'EBA Calls on National Authorities to Take Supervisory Actions for the Removal of Obstacles to Account Access under the Payment Services Directive', *European Banking Authority* (Web Page, 22 February 2021) <https://www.eba.europa.eu/eba-calls-national-authorities-take-supervisory-actions-removal-obstacles-account-access-under>. See also TrueLayer (n 86) 10.

208 James Eyers, 'Loan Process Stripped Back by Open Banking', *The Australian Financial Review* (Sydney, 12 April 2022).

209 TrueLayer (n 86) 11.

210 *Statutory Review of the Consumer Data Right* (n 119) recommendation 2.1.

211 Australian Government, *Government Statement in Response to the Statutory Review of the Consumer Data Right* (Government Response, June 2023) 6. See also Australian Government, *Screen Scraping – Policy and Regulatory Implications: Discussion Paper* (August 2023) 3 <https://treasury.gov.au/sites/default/files/2023-08/c2023-436961-dp.pdf >.

212 Ibid.

VI Conclusion

SS has mattered historically. At the dawn of the FinTech industry, many businesses facing the unwillingness of incumbents to share customer data were forced to choose between SS and having no data access. Understandably, they chose SS. Had FinTechs waited for the banking industry to develop and open their APIs, there may have been no FinTech sector in Australia at all or it may well have had far fewer compelling products and services to offer.

As shown in this article, many FinTechs and data aggregators associate SS with business convenience, efficiency and low costs. They argue they serve their customers by eliminating the need for tedious manual data sharing and offering more reliable services, as SS cannot be blocked by account-holding institutions as readily as can data access via APIs. Crucially, however, SS gives these businesses control over when and how much data to scrape and allows them to exploit the data primarily for their own benefit rather than for the benefit of consumers. By avoiding CDR accreditation requirements, proponents of SS have a lower regulatory burden than businesses using the CDR. Not least for this reason, preserving the current hybrid model — where data can be derived from either SS or APIs — appeals strongly to many screen scraping businesses. They argue the technology should, at the minimum, be retained as a redundancy fail-safe for when APIs are not working.

The arguments against SS, in our opinion, are far more persuasive. SS remains an innately dangerous online practice, which gives third parties virtually unrestricted access to, and control over, customers' financial accounts. These customers are at an increased risk of digital fraud and of forfeiting their protections under the E-Payments Code. The government repeatedly warns consumers to protect and not hand over their online user credentials to third parties.[213] With more than 80 per cent of Australians preferring to bank online,[214] it is inconsistent and dangerous to allow Australian FinTechs to actively encourage customers to ignore this advice.[215]

From a technical perspective, SS is a slow and unreliable method of data collection, which has traditionally been employed due to the lack of a better alternative, but which is now long overdue for retirement.

---

213 'Do not share your passphrases with anyone and be aware of your surroundings when using them in public': Australian Cyber Security Center, 'Creating Strong Passphrases', *Australian Signals Directorate* (Web Page, October 2021) <https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases>. '[D]on't share your myGov sign in details with anyone': Australian Government, 'How You Can Protect Your MyGov Account', *myGov* (Web Page, 27 October 2022) <https://my.gov.au/en/about/privacy-and-security/security/how-you-can-protect-your-mygov-account>.

214 Australian Banking Association, 'Banking Customers Continue Shift to Digital', *Australian Banking Association* (Web Page, 19 October 2021) <https://www.ausbanking.org.au/banking-customers-continue-shift-to-digital/>.

215 See also Financial Rights Legal Centre and the Consumer Action Law Centre (n 40) 14.

From a consumer perspective, SS encourages unsafe data practices by consumers and harms many directly, as it enables payday lenders to target specific consumers precisely when they are most acutely financially vulnerable, pushing them into unsustainable spirals of debt.

From a business perspective, SS enables an inertia that, in the longer term, will not serve commerce or the broader economy in Australia. FinTechs and others will continue to rely on SS from this inertia and their unwillingness to make the investment required to be accredited under the CDR. This will inevitably slow the take up of the CDR. Yet the CDR is one of Australia's most ground-breaking and important reforms.

Throughout history, water and sanitation engineers have saved more lives than the medical profession. When fully rolled out and operational, the CDR will safely deliver the water the modern economy requires to thrive, which is data, and will impose hygiene standards upon the businesses that, as accredited data recipients, hold the data.[216] SS will delay the rollout of a world-leading reform, which in time will offer much to the living standards of all Australians.[217]

---

[216] Natalia Jevglevskaja and Ross P Buckley, 'A World-Leading Sanitation System for Our Digital Economy: The Consumer Data Right' (2023) *Australian Business Law Review* (forthcoming).

[217] Jevglevskaja and Buckley, 'The Consumer Data Right' (n 158).