LexisNexis

Australian
Banking & Finance Law Bulletin

2021 . Vol 37 No 2

Contents

Information contained in this newsletter is current as at May 2021

LexisNexis Butterworths

Australian
Banking & Finance
Law Bulletin

General Editor's note

Karen Lee *LEGAL KNOW-HOW*

The Financial Sector Reform (Hayne Royal Commission Response) Bill 2020 (Cth) passed both Houses on 10 December 2020, and was assented to on 17 December 2020. The legislation gives effect to recommendations 1.6, 2.8 and 7.2 of the Financial Services Royal Commission by clarifying and strengthening the breach reporting regime for Australian financial services licensees, introducing a comparable breach reporting regime for Australian credit licensees, and requiring financial services licensees and credit licensees to report serious compliance concerns about financial advisers and mortgage brokers respectively. The new breach reporting obligations will commence operation on 1 October 2021. I have the perfect article to help banking and finance lawyers prepare for the changes — "Warning: Do not breach your breach reporting obligations" is by **Andrea Beatty**, **Chloe Kim** and **Shannon Hatheier** (Piper Alderman). The authors cover a lot of ground. Among other things, they explain the obligations, including the controversial "dobbing" obligation, and important concepts, including the significance test and the meaning of "reasonable grounds".

Did you know there are many overlapping doctrines that come into play in an insolvency when parties have contributed variously, and at different times, to augment a common fund? "Insolvency set-off, subrogation, and the rule in *Cherry v Boultbee*[1] — equity (or common sense) in action in the protection of secured assets" is the next article in this edition of the *Australian Banking and Finance Law Bulletin*, by **Associate Professor Lee Aitken** (University of Newcastle). Lee explains the widely applied "rule" in *Cherry v Boultbee*, and its most recent application in *Re Force Corp Pty Ltd (in liq)*,[2] in the context of a liquidation set-off arising from payments made pursuant to the priority creditor provisions of the Corporations Act 2001 (Cth). In his decision, Gleeson J dealt with (among other things) subrogation and insolvency set-off under s 533C of the Corporations Act. As always, Lee's analysis, commentary and insights are valuable, and I thank Lee for his ongoing contribution to help keep banking and finance lawyers stay current in our practice area.

Last but certainly not least, I am delighted that **David Kreltszheim** (Cornwalls) is writing for our readers again. His latest article is "The 'consumer data right (CDR) as a service' for Australian FinTechs: a workable way out of a scrape". David suggests a working model for "CDR as a Service". This is very interesting, and David's analysis and insights make his article a great read. I am not going to give too much away by saying more!

Karen Lee
Principal
Legal Know-How
karen.lee@LegalKnowHow.com.au

Karen Lee is the General Editor of the Australian Banking & Finance Law Bulletin and the Financial Services Newsletter. She also partners with LexisNexis in other capacities, including as Specialist Editor for precedents in banking and finance, mortgages and options, and as contributing author of a number of other publications, including Australian Corporation Finance Law, Halsbury's Laws of Australia and Practical Guidance General Counsel. Karen established her legal consulting practice, Legal Know-How, in 2012. She provides expert advice to firms and businesses on risk management, legal and business process improvement, legal documentation, regulatory compliance and knowledge management. Prior to this, Karen worked extensively in-house, including as Head of Legal for a leading Australasian non-bank lender, as well as in top-tier private practice, including as Counsel at Allen & Overy and Clayton Utz.

Footnotes

1. *Cherry v Boultbee* (1839) 4 My & Cr 442; 41 ER 171.
2. *Re Force Corp Pty Ltd (in liq)* (2020) 149 ACSR 451; [2020] NSWSC 1842; BC202012634.

Warning: Do not breach your breach reporting obligations

***Andrea Beatty**, **Chloe Kim** and **Shannon Hatheier** PIPER ALDERMAN*

The Financial Sector Reforms (Hayne Royal Commission Response) Act 2020 (Cth) (FSR Act) was assented to on 17 December 2020 and carried into effect a host of reforms which will greatly impact the financial services industry. The reforms include measures designed to strengthen the Australian Financial Services Licence (AFSL) breach reporting regime and require Australian Credit Licence (ACL) holders to commence breach reporting under the National Consumer Credit Protection Act 2009 (Cth) (NCCP Act). The new breach reporting obligations will commence operation on 1 October 2021.

Breach reporting obligations

The reforms were introduced to address the following two recommendations in the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry's Final Report*:[1]

- Recommendation 2.8: All AFSL holders should be required, as a condition of their licence, to report "serious compliance concerns" about individual financial advisers to Australian Securities and Investments Commission (ASIC) on a quarterly basis.
- Recommendation 7.2: The recommendations of the ASIC Enforcement Review Taskforce made in December 2017 that relate to self-reporting of contraventions by financial services and credit licensees should be carried into effect.

The FSR Act will overhaul the current AFSL breach reporting regime and implement more prescriptive requirements as to what amounts to a reportable breach and when such breaches should be reported. ACL holders will equally be required to adhere to the new regime albeit for the first time.

The reforms draw upon the recommendations of the ASIC Enforcement Review Taskforce (ASIC Taskforce) which highlighted the apparent inadequacy of the existing Compliance Certificate regime for ACL holders, describing it as "no substitute for the self-reporting obligation that AFS licensees are subject to."[2] The ASIC Taskforce further proposed a host of recommendations aimed at reforming the significance test, clarifying reportable situations and extending the reporting period, all of which have been carried into effect by the FSR Act.

AFSL significance test

Under the new AFSL breach reporting regime, a reportable obligation will arise when a licensee or representative has breached a core obligation or can no longer comply with a core obligation and the breach is or will be significant. Core obligations are specified in the FSR Act and include, among other provisions, the obligation to act "efficiently, honestly and fairly"[3] as well as the prohibitions on unconscionable, misleading and deceptive conduct.[4]

The FSR Act introduces a dual part test for determining significance, the first of which deems a breach of a core obligation significant if any of the following circumstances apply:

- the provision breached may involve imprisonment for a term of 3 months or more if the offence involves dishonesty or 12 months or more in any other case
- the provision breached is a civil penalty provision, s 1041H(1) of the Corporations Act 2001 (Cth) or s 12DA(1) of the Australian Securities and Investments Commission Act 2001 (Cth) or
- the breach results, or is likely to result, in material loss or damage to clients or members

The second test is whether a breach or likely breach of a core obligation will be significant having regards to the following factors:

- the number and frequency of similar previous breaches
- the impact of the breach or likely breach on the licensee's ability to provide financial services covered by the licence and
- the extent to which the breach or likely breach indicates that the licensee's arrangements to ensure compliance with those obligations are inadequate

The prescriptive nature of the revised significance test will likely expand the scope of circumstances in which a breach report is required. The government has recognised this concern and plans to revisit the significance test should ASIC receive a large number of "unproblematic breach reports for minor, technical or inadvertent breaches of civil penalty provisions."[5]

Time frames

As suggested by the ASIC Taskforce, licensees will now be required to lodge a report with ASIC within 30 days from when the licensee first knows, or is reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen in relation to the licence.[6] The extension of the reporting period from 10 to 30 days is intended to reflect stakeholder submissions to the effect that licensees generally require more than 10 days to sufficiently investigate a matter and determine whether a significant breach has occurred. Licensees will also be required to report an investigation where it continues for more than 30 days and report the outcome of an investigation within 10 days of its determination.

Reasonable grounds

Under the FSR Act, licensees have an obligation to lodge a report with ASIC if there are *reasonable* grounds to believe that a reportable situation has arisen. The phrase "reasonable grounds to believe", though not defined in the FSR Act, is described in the Explanatory Memorandum[7] as clarifying that breach reporting obligations are to be assessed objectively. While it has the appearance of being an objective test the provision includes reference to "knowledge" and "recklessness" which are inherently subjective in nature. The interpretation of the provision is therefore unclear and further complicates the remaining issue of a corporation's scope of knowledge.

The knowledge of a body corporate is generally attributed to the "directing mind and will" of the corporation,[8] such that members of the board and senior officers will be regarded as embodying the corporation's knowledge. However, what is less clear is the circumstances in which a body corporate will be held accountable for reportable breaches at lower levels of management. To avoid this uncertainty, licensees should ensure adequate systems and procedures are in place to funnel issues to top management.

ACL regime

As stated above, the FSR Act will introduce an ACL breach reporting regime that mirrors the amended regime for AFSL holders. ACL holders will similarly be subject to a dual part significance test, in which a breach of a "key requirement" under the National Credit Code will be deemed significant. ACL holders will however be exempt from reporting where an auditor or actuary of the licensee has provided the Australian Prudential Regulation Authority a written report about a reportable situation within 10 business days of the licensee knowing that, or is reckless with respect to whether, there are reasonable grounds that a reportable situation has arisen. This is intended to avoid overlaps between the matters required to be reported under the NCCP Act and other legislation.

Dobbing

The FSR Act also introduced what has been referred to as the "dobbing" obligation, which requires licensees to lodge a report with ASIC within 30 days after first reasonably knowing that there are reasonable grounds to suspect that a reportable situation has arisen about an individual who:

- provides personal advice to retail clients about relevant financial products and is operating under another AFSL or
- is a mortgage broker operating under another ACL

This new requirement goes beyond the obligation to report the licensee's own conduct and extends to reporting misconduct by financial advisers working under other AFS and credit licensees. While the obligation imposes a lower threshold, requiring licensees to have reasonable grounds to suspect rather than reasonable grounds to believe, licensees will now need to consider whether they have adequate systems in place to alert them to a reportable situation when dealing with independently licensed financial advisors and mortgage brokers.

Contravention

Licensees should be particularly cognisant of the significantly higher civil penalties for non-compliance under the reformed breach reporting regimes. Individuals who fail to lodge a report with ASIC may incur a penalty of up to $1,110,000 (5000 penalty units) or a term of imprisonment of up to 2 years.[9] Alternatively bodies corporate may face a penalty anywhere between a minimum of $11,100,000 (50,000 penalty units) to a significant $555,000,000 (2,500,000 penalty units).[10]

Regulations

On 10 March 2021, Treasury released draft regulations intended to clarify the breach reporting regimes. The draft regulations prescribe a list of civil penalty provisions contained in the Corporations Act and NCCP

Act that will not be taken to be significant if contravened and therefore may not need to be reported. The regulations importantly narrow the scope of reportable situations under the new regime, largely doing away with the requirement to report breaches of trivial civil penalty provisions.

As stipulated in the draft regulations, civil penalty provisions under the Corporations Act that will not be taken to be significant if contravened by an AFSL include, among others, failing to give a Product Disclosure Statement when giving personal financial advice[11] and providing a defective disclosure document or statement.[12] Similarly for ACL holders, a failure to cite the licensee's ACL number,[13] among other civil penalty provisions in the NCCP Act, will not be taken to be significant if breached.

The regulations further specify that AFSL and ACL holders are not required to pay a fee on lodging a breach report so as to not deter self-reporting.

Key takeaway

With the new breach reporting regime scheduled to commence on 1 October 2021, licensees should be preparing well in advance of the commencement date. The complexity and scope of the new regime will no doubt enhance the time and effort required to update licensee's internal systems and guidance to ensure compliance. Given the hefty penalties for non-compliance there is no room for licensees to be taking chances.

AFSL holders must update their breach reporting policies whilst ACL holders should prepare breach reporting policies. All licensees must train staff likely to be impacted by the new obligations.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeaty.com.au

Chloe Kim
Lawyer
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

Shannon Hatheier
Law Clerk
Piper Alderman
shatheier@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. The Treasury *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry's Final Report* (2019).
2. Australian Government *ASIC Enforcement Review Taskforce Report* (December 2017) p 7.
3. Corporations Act 2001 (Cth), s 912A(1)(a).
4. Australian Securities and Investments Commission Act 2001 (Cth), ss 12CA, 12CB and 12DA(1).
5. Explanatory Memorandum, Financial Sector Reform (Hayne Royal Commission Response) Bill 2020 (Cth) cl 11.140.
6. Above n 3, s 912DAA(1) and NCCP Act, s 50B(1).
7. Above n 5, cll 11.39–11.40 and 11.60–11.62.
8. *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153 [1971] All ER 127.
9. Above n 3, s 1317G(3) and NCCP Act s 167B(1).
10. Above n 3, s 1317G(4) and NCCP Act s 167B(2).
11. Above n 3, s 1012A(5).
12. Above n 3, s 1021E(8).
13. NCCP Act, s 52(2).

Australian
Banking & Finance
Law Bulletin

Insolvency set-off, subrogation and the rule in Cherry v Boultbee — equity (or common sense) in action in the protection of secured assets

Lee Aitken *UNIVERSITY OF NEWCASTLE*

Professor Harold Laski reported an apothegm of Sir George Jessel MR — that no-one can understand the rules of equity until they are at least 40! But equity is just applied common sense.

If, for example, you want to take something out of a common fund, you have to put back in any previous payments you have received from it — otherwise you are "double dipping".

Equally, if X's assets are used to discharge Y's (statutory) liability, fairness by way of subrogation demands that X may stand in Y's shoes to recover from a fund which may be available to satisfy that demand.

What then is the position if certain statutory priority creditors under the Corporations Act 2001 (Cth) have their entitlements discharged by way of a payment from the assets of a secured creditor?

What is subrogation?

In *Blakely, Re Akron Roads Pty Ltd (in liq)* Anderson J said:

> Subrogation is the transfer of rights from one person to another without assignment or assent of the person from whom the rights are transferred . . . unconscionability is the rubric on which equitable subrogation is built. An equitable right of subrogation as a remedy should be based on well-settled principles and available in defined circumstances that make it unconscionable for the defendant to deny the proprietary interest claimed by the plaintiff.[1]

The "rule" in Cherry v Boultbee

The rule in *Cherry v Boultbee*[2] is widely applied, principally in distributing testamentary, or bankrupt, estates:[3]

> The rule in *Cherry v Boultbee* is applied in equity to the distribution of a fund. Put very shortly (at this stage) equity requires that a person cannot share in a fund in relation to which he is also a debtor without first contributing to the whole by paying his debt. The operation of the rule may be illustrated by an example. Suppose A is indebted to B in the sum of £1,000. B dies leaving his residuary estate to be shared equally amongst four beneficiaries, of which A is one. After the payment of B's debts, administration expenses and specific legacies (but before A has paid the £1,000) the amount of the residuary estate in the hands of B's executors is £10,000. A must bring his debt into account before he can receive his share. So the amount which he will receive will be £1,750 (1/4 of {£10,000 + £1,000} – £1,000). The other three beneficiaries will each receive £2,750. It can be seen that, if A's debt were greater than his aliquot share of the whole, he would receive nothing in the distribution.[4]

The most recent decision: Re Force Corp Pty Ltd (in liq)

The "rule" has been discussed most recently in detail by Gleeson J in *Re Force Corp Pty Ltd (in liq)*[5] (*Force Corp*) in the context of a liquidation set-off arising from payments made pursuant to the priority creditor provisions of the Corporations Act. In addition, his Honour dealt with subrogation, and equitable, and insolvency set-off under s 533C of the Corporations Act.

By way of background, it is relevant to note the operation of s 433 of the Corporations Act which provides for certain classes of creditors (including employees) to receive a priority payment out of "circulating assets" security as defined by s 340 of the Personal Property Securities Act 2009 (Cth).

As Gleeson J noted, the legislation is designed to meet what Lord Macnaghten stigmatised in *Salomon v A Salomon & Co Ltd*[6] as "a great scandal" — the widespread use of floating charges over trading stock, book debts and other circulating capital:

> . . . which produced a situation in which a company's business might appear to be thriving and employees and ordinary trade creditors dealt with it on that basis unaware of the existence of a floating charge.[7]

Once the charge crystallised, the debenture-holders would swoop down like the wolf on the fold and seize everything.

The legislative response was to carve out the circulating assets from those covered by a fixed charge and make the proceeds from realising them in the company. Employees, in particular, are to be protected because their efforts have gone to fructify the assets covered by the creditor's security.[8]

No obligation to "segregate" secured assets

In dealing with the circulating assets, the receiver is not:

> . . . obliged to effectively segregate or trace the proceeds of circulating assets and to pay employees from assets of that type, as opposed to making the payment from other funds that can later be augmented by the recovery of circulating assets.[9]

As Bryson J (as he then was) noted in *Whitton v ACN 003 266 886 Pty Ltd (in liq) (formerly Boswell Printing Pty Ltd)*[10] to require otherwise might tear the heart out of the company as a going concern by forcing the immediate realisation of assets necessary to its continued trading.

That possibility raises a timing issue since it is possible (indeed likely) that the secured creditor's assets will be used first since they are the most readily available for realisation. In such a situation, does the secured creditor lose its rights entirely, or is it subrogated to those employees (or other preferred) creditors who have had the benefit of its secured assets?

If a secured creditor has its security diminished because its assets are used to pay the employees out of circulating assets that form part of the secured property, it is entitled to be subrogated to the position of those employees who have received payment.[11]

The role of insolvency set-off, equitable set-off or Cherry v Boultbee?

But is that entitlement in itself to be diminished in the light of insolvency set-off or the rule in *Cherry v Boultbee*?

In *Force Corp*, broadly speaking, the receivers had recovered $1.4 million from the company's circulating assets but only about $850,000 was paid by the receivers to the statutory priority creditors (the Australian Taxation Office (ATO), the employees, and superannuation funds). Thus, some $540,000 was used by the receivers and paid for the benefit of the secured creditor, Lease Collateral Pty Ltd (Lease Collateral), in breach of the statutory obligation under s 433(3)(c) of the Corporations Act. Consequently, the receivers were liable to restore this to the company.[12]

The liability of the secured creditor?

The liquidators contended that Lease Collateral would also be liable to Force Corp Pty Ltd (Force Corp) either because it was an "accessory" to the contravention by the receivers, or on a restitutionary basis as a party which had received funds mistakenly in breach of a statutory duty (viz under s 433):

> Where money is paid by reason of mistake, the payer may recover it from the recipient in a common law action for money had and received: *Australian Financial Services Leasing Pty Ltd v Hills Industries Ltd* (2014) 253 CLR 260 at 568. Although recovery by the claimant may depend upon whether it would be inequitable for the recipient to retain the benefit, it is not necessary for the claimant to allege or prove that the retention of the money received by the defendant would be unjust as that is a matter on which the defendant bears the onus: *Hills Industries* at 593.[13]

Was Lease Collateral entitled to set-off the amount it received via the subrogated payment, against its liability for the liability as an "accessory" or payee by way of mistake?

Insolvency set-off under s 553C of the Corporations Act

Gleeson J discussed the operation of insolvency set-off in detail.[14] The object of set-off under the Corporations Act is to do substantial justice between the parties — the doctrine should thus be given its widest possible scope.[15] The set-off is "self-executing"; it operates automatically from the winding up to extinguish mutual claims then in existence.[16] The relevant date for the assessment whether a set-off exists is when the admissibility of a claim to proof is determined.[17] The relevant "account" which is to be struck under s 553C "is deemed to be taken . . . as at the date of the winding up" when "the respective claims cease to have a separate existence as choses in action, and are replaced by a claim to a net balance".[18] Debts available to be set-off in respect of mutual dealings include those then due and debts which are then contingent but ultimately mature into pecuniary demands. A debt is "contingent" if:

> . . . as a result of an existing obligation, the company will be liable to pay or be entitled to receive a sum of money on the occurrence of a future event which may happen, not which must happen.[19]

Here it was said that the "debt" was relevantly contingent — it was said there was an analogy with a liquidator's statutory recovery claims.[20] (Part of the problematic cases therein discussed seem to involve a notion first propagated in obiter dicta by Young JA in *Buzzle Operations Pty Ltd (in liq) v Apple Computer Australia Pty Ltd*[21] that a court-appointed liquidator could not be allowed to act "inequitably".[22])

But in this case there was no "mutual debt" or "mutual dealings" between the secured creditor and Force Corp which might satisfy s 553C since the benefit conferred by definition occurred after the commencement of the winding up.[23] In any event, even if that view were wrong, there was notice of insolvency sufficient to preclude the operation of s 553C.[24]

Equitable set-off?

Were the two rights (to repay the money, and to receive the subrogated amount) so intertwined or inextricably bound up that it would be "unconscionable" not to take one into account without the other?[25] Gleeson J did not think so — here there was no "counter-claim which goes to the root of, and impeaches the title of Force Corp's restitutionary claim against Lease Collateral" in relation to the latter's mistaken receipt.[26]

Cherry v Boultbee?

Cherry v Boultbee will only apply if "insolvency set-off" is not available.[27] The rule is best described as a right to appropriate a particular asset as payment, as opposed to a right of set-off or a right of retainer.[28] It requires a netting-off of reciprocal monetary obligations.[29] Gleeson J made appropriate orders to reconcile the payments which had been made as sought by the liquidators.[30]

Conclusion

The decision repays close reading and illustrates the multiplicity of overlapping doctrines which come into play in an insolvency when parties have contributed variously, and at different times, to augment a common fund. The position is made more complex because of the restrictions which hedge the direct operation of statutory set-off under s 553C which then throw the parties back on broad equitable doctrines to ensure that "he who seeks equity, must do equity".

Lee Aitken
Associate Professor
University of Newcastle
lee.aitken@newcastle.edu.au
www.newcastle.edu.au

Footnotes

1. *Blakely, Re Akron Roads Pty Ltd (in liq)* [2020] FCA 1378; BC202009275 at [26].
2. *Cherry v Boultbee* (1839) 4 My & Cr 442; 41 ER 171 as explicated in *Re Melton; Milk v Towers* [1918] 1 Ch 37.
3. See, generally, L Aitken "Recent applications of the rule in *Cherry v Boultbee* (or *Jeff v Woods*)" (2010) 84(3) *Australian Law Journal* 191, an article which has been overtaken by recent authority now discussed.
4. *Re SSSL Realisations (2002) Ltd (in liq); Re Save Group plc (in liq)* [2006] 2 WLR 1369; [2006] Ch 610 at [12] per Chadwick LJ.
5. *Re Force Corp Pty Ltd (in liq)* (2020) 149 ACSR 451; [2020] NSWSC 1842; BC202012634. His Honour was sitting in the Equity-Corporations List.
6. *Salomon v A Salomon & Co Ltd* [1897] AC 22 at 53.
7. Above n 5, at [44].
8. *Stein v Saywell* (1969) 121 CLR 529 at 544 per Barwick CJ; 550 per McTiernan and Menzies JJ. See the authority cited by Gleeson J, above n 5, at [45] culminating most recently in *Kirman v RWE Robinson and Sons Pty Ltd (in liq), Re RWE Robinson and Sons Pty Ltd (in liq)* [2019] FCA 372 at [40].
9. Above n 5, at [52].
10. *Whitton v ACN 003 266 886 Pty Ltd (in liq) (formerly Boswell Printing Pty Ltd)* (1996) 42 NSWLR 123 at 137.
11. Corporations Act 2001 (Cth), s 433(3)(c); above n 5, at [64] citing above n 1, at [30]–[34].
12. Above n 5, at [72] citing inter alia, above n 10, at 137B.
13. Above n 5, at [73], per Gleeson J. On this second limb, Gleeson J observed (at [74]).
14. Above n 5, at [80]–[100].
15. Above n 5, at [79].
16. Above n 5, at [81].
17. Above n 5, at [82].
18. Above n 5, at [83].
19. Above n 5, at [84].
20. *Hussain v CSR Building Products Ltd, Re FPJ Group Pty Ltd (in liq)* [2016] FCA 392; 112 ACSR 507; [2016] FCA 392; BC201603630 at [227].
21. *Buzzle Operations Pty Ltd (in liq) v Apple Computer Australia Pty Ltd* (2011) 81 NSWLR 47; 277 ALR 189; [2011] NSWCA 109; BC201103281 at [279].
22. See above n 5, at [90]–[98] discountenancing this reasoning.
23. Above n 5, at [100].
24. Above n 5, at [101]–[107].
25. Above n 5, at [111]–[112].
26. Above n 5, at [113].
27. Above n 5, at [116].
28. Above n 5, at [117] where his Honour is quoting from his earlier discussion in *Re Hawden Property Group Pty Ltd (in liq) (ACN 003 528 345)* (2018) 125 ACSR 355; [2018] NSWSC 481; BC201802923 at [37]–[43].
29. Above n 5, at [118].
30. Above n 5, at [119]–]123].

Australian
Banking & Finance
Law Bulletin

The "consumer data right (CDR) as a service" for Australian FinTechs: a workable way out of a scrape

David Kreltszheim *CORNWALLS*

Australia's consumer data right regime[1] (CDR Regime) as it applies in the banking sector[2] is intended to give CDR "consumers" (broadly, any individual or company having a specified type of account with a bank):

> . . . greater access to and control over their data. It will improve consumers' ability to compare and switch between products and services, and will encourage competition between service providers, leading not only to better prices for customers but also more innovative products and services.[3]

This is truly exciting reform that has been consistently advanced since 2018.[4] There have been some delays in the phased "go live" dates for the reform but in my view this is understandable given the magnitude and complexity of the reform. Further, at every stage, policy makers need to manage the tension between promoting competition and innovation on the one hand and maximising consumer safety, confidentiality and privacy on the other. This tension is why it is taking time to develop a workable model for start-up FinTechs[5] — and established but small FinTechs — to have the benefit of "CDR as a Service" as a relatively quick and cost-effective way to participate in the CDR Regime. I suggest that Australia is now no more than 2 years away from developing this model.

In the meantime, many Australian FinTechs are unable or unwilling to take the time, and incur the expense, to become accredited data recipients under the CDR Regime. It is estimated to cost as much as AUD$250,000 to complete an application to become an accredited data recipient (ADR) at the only level that is presently available, that is, the "unrestricted" level.[6] Further, the Australian Competition and Consumer Commission (ACCC) estimates that it costs in the vicinity of AUD$50,000 to AUD$70,000 just to set up a data storage centre for storing CDR data.[7]

Therefore, for now, many FinTechs continue to use alternative data capture mechanisms to offer their services. Those alternative mechanisms include "screen scraping" and — for bigger players like the providers of business and accounting platforms — direct data feeds negotiated on a bilateral basis between service providers and Australian banks. In the banking context, "screen scraping" — or the less harmful sounding "digital data capture" — refers to the practice of an organisation (like a FinTech, a bank — say bank B — or a data aggregator) using a customer's login details to access the customer's bank accounts with bank A in order to provide a secondary product or service. This sometimes happens on an ongoing basis and at other times on a one-off basis. This technology is widely used by banks, lenders, financial management applications, personal finance dashboards and accounting products.[8]

Accredited data recipients under the CDR Regime

The CDR Regime, as it applies in the banking sector, permits an ADR such as a FinTech to receive a CDR consumer's CDR data from a data holder (the CDR consumer's bank) with the consent of that CDR consumer. Broadly, "CDR data" in the banking sector includes customer data, account data and transaction data in relation to a range of bank accounts.[9] An ADR must obtain a consumer's consent before requesting the consumer's CDR data from the consumer's bank. That consent must be voluntary, express, informed, specific as to purpose and time-limited (to a maximum period of 12 months unless withdrawn earlier).[10] Further, the bank must ask the consumer to authorise the bank to disclose the applicable CDR data to the ADR.[11]

An ADR is subject to privacy[12] rules about how it handles CDR data.[13] Amongst other things, the ADR must establish a formal governance framework for managing information security risks relating to CDR data setting out the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security. An ADR must also assess, define and document the boundaries of its "CDR data environment", that is, the information technology systems used for, and processes that relate to, the management of CDR data. An applicant for accreditation as an ADR must provide evidence to demonstrate that it satisfies the detailed security requirements about the security of CDR data. This evidence includes an IT security assurance report prepared in accordance with specified standards or evidence that the applicant has ISO 27001 certification.[14]

A working model for "CDR as a Service"

I suggest a working model for "CDR as a Service" with the features set out below. These features combine proposals made in the Government's CDR Rules Expansion Consultation Paper of September 2020 (CDR Expansion Consultation Paper),[15] submissions made by prospective intermediaries in October and November 2020 in response to that Consultation Paper,[16] and the CDR Future Directions Report publicly released in December 2020.[17] The features of this working model do not correspond exactly with any particular proposal.

- An organisation (A) which has the highest level of accreditation as an ADR (unrestricted) may "sponsor" an affiliate/authorised representative (B).
- That sponsorship may involve the enrolment of B as an ADR at a lower level of "affiliate accreditation" from the regulator[18] or B will be enrolled as an authorised representative of A. It will be relatively less costly and quicker for B to be sponsored in this way, amongst other things reflecting that B will not need to obtain an IT assurance report and satisfy the other costly and time consuming IT-related conditions that are required for an "unrestricted" ADR accreditation. The enrolment of B will record that A is B's sponsor and that B is an affiliate/authorised representative of A.
- A is responsible for policing B's handling of CDR data, including by reviewing B's risk, security and privacy controls. This includes an initial review to confirm the adequacy of those controls prior to A certifying that B is permitted to be A's affiliate or authorised representative and ongoing monitoring of those controls for so long as B is an affiliate or authorised representative sponsored by A.
- A will be required to provide a regular certification to the regulator about the affiliates or authorised representatives (like B) that are sponsored by it, and A will be subject to additional liability under the CDR Regime as a result of providing that certification.[19] In support of this certification function, A must have:

  > . . . a demonstrably mature third-party governance [program] integrated with [its] overall risk management program . . . This is not simply a point-in-time assessment or attestation, but rather a comprehensive set of preventative, detective and response controls implemented in the initial due diligence, onboarding and duration of the . . . relationship [between A as sponsor and B as A's affiliate or authorised representative]".[20]

- As an ADR (although with an "affiliate accreditation" and not an "unrestricted" accreditation) or an authorised representative of A, B will be subject to the obligations imposed on affiliate ADRs or authorised representatives under the CDR Regime. These include obligations relating to seeking consent, deletion and de-identification of CDR data.[21] A will most likely provide B with the technical infrastructure to comply with these obligations, potentially by means of features that are "white-labelled", ie provided by A but with B's branding.
- A can sponsor multiple affiliates or authorised representatives, subject to the approval of the regulator of each application for affiliate accreditation or appointment of an authorised representative.
- B must disclose to CDR consumers that B is an affiliate or authorised representative of A.

I have described the above model as "CDR as a Service" because it is loosely analogous to "software as a service": in the same way that software as a service removes the need for organisations to install and run applications within their own IT environment, this model enables affiliates or authorised representatives like B to rely on intermediaries like A for a significant portion of the infrastructure that B needs in order to handle CDR data in accordance with the CDR Regime. It is a loose analogy because B will have obligations in its own right under the CDR Regime, either as an ADR (although with an "affiliate" accreditation and not an "unrestricted" accreditation) or as an authorised representative of A.

Will the "CDR as a Service" model (or a variant of it) be accepted?

The CDR as a Service model, or any variant of it, has not been accepted as of the end of March 2021. The last 6 months has been a period of intense regulatory review and lobbying activity as various CDR intermediary models have been considered in detail by the Australian Government. There is a lot at stake. What follows are snapshots from publicly available materials that have been released on this topic in the 6 months from the end of September 2020 up to the end of March 2021.

CDR Expansion Consultation Paper: September 2020

This Consultation Paper recognised that:

> For the consumer benefits of the CDR to be fully realised, it is critical for there to be a broad range of accredited data recipients participating in the system . . . to achieve the

> competition and innovation objectives of the regime, and for the CDR to support Australia's digital economy. [The Australian Government] wants to support participation from entities that may not be able to meet the requirements for accreditation [at the "unrestricted" level] having regard to the nature of their business or the type of data they seek to access . . . The three kinds of restricted accreditation in the proposed rules are the *limited data restriction*, the *data enclave restriction* and the *affiliate restriction*. The proposals aim to lower barriers to entry by reducing some of the upfront and ongoing costs of accreditation as compared to the unrestricted level, while maintaining appropriate information security and consumer protections.[22] [Emphasis added.]

As noted above, the Consultation Paper proposed three kinds of restricted accreditation that would be easier to obtain than the "unrestricted" accreditation:

- *Limited data accreditation*: this accreditation is for applicants who wish to handle CDR data that has been assessed as lower risk compared to the complete range of data that is in scope and able to be handled by ADRs with an unrestricted accreditation.[23]
- *Data enclave restriction*: this accreditation is for applicants who will work with higher risk data sets behind the data security firewalls of higher tier accredited parties. Those higher tier accredited parties will be those who have established a "data enclave". The applicant who is subject to a data enclave restriction will not be able to access the relevant data outside the enclave or download local copies of the data to another environment.[24]
- *Affiliate restriction*: this accreditation is for applicants who have a commercial relationship with an ADR with an unrestricted accreditation. That ADR would "sponsor" the applicant into the CDR Regime by certifying that sponsor is satisfied that the applicant meets the accreditation criteria that need to be complied with by an affiliate.[25] This model is closest to the "CDR as a Service" model outlined above.

Submissions in response to the CDR Expansion Consultation Paper: October/November 2020

Over 50 Submissions made in response to the CDR Expansion Consultation Paper have been made publicly available by the ACCC.[26] Several regulators, banks, prospective intermediaries (sponsors), FinTechs, industry associations and consumer advocates have expressed concern about the complexity of the proposals outlined in the CDR Expansion Consultation Paper.[27] Prospective sponsors generally endorsed the affiliate restriction (thereby favouring a form of "CDR as a Service" model).[28] However, for reasons that are examined later in this article, one prospective sponsor strongly challenged the model under which sponsors would be responsible or liable for the acts or omissions of affiliates sponsored by it in relation to the affiliates' handling of CDR data.[29]

Public release of the "CDR Future Directions" Report: December 2020

The following recommendations in the CDR Future Directions Report[30] are relevant to the increase of participation in, and access to, the CDR system by means a "CDR as a Service" mechanism or a variant of it:

- *Authorised representatives*:

  > CDR data should be able to be released to a CDR-authorised representative of an accredited data recipient, with the customer's consent. The authorised representative should be able to hold a lower tier of accreditation, in light of the principal accredited data recipient providing data access, taking on liability for Consumer Data Right compliance and taking on responsibility for putting in place arrangements to ensure compliance. The design of arrangements should have close regard to the role of authorised representatives under the Australian financial services licensing regime.[31]

- *Providing data outside the CDR system to regulated parties*:

  > The Consumer Data Right should allow regulated third parties operating outside the Consumer Data Right ecosystem to receive varying levels of data with the consent of the consumer, with reference to the level of regulation of the recipient. This access should include transfers of CDR data or derived data for regulated activities or for regulatory compliance activities at the customer's direction.[32]

  The regulated third-party receiving data from the accredited data recipient may be the consumer's:[33]

  — lawyer or financial adviser receiving the consumer's financial data
  — accountant receiving the consumer's accounting data
  — mortgage broker receiving data feeds to generate analyses and pre-fill forms, or
  — prospective lender (not accredited in the CDR Regime) receiving income and expense verifications

- *Insights for non-accredited persons*:

  > The Consumer Data Right should allow non-accredited third parties operating outside the Consumer Data Right ecosystem to receive, from a [bank] or accredited data recipient, lower risk insights data derived from CDR data.[34]

  This would be to fulfil a particular purpose (sole purpose) mandated by a consumer and could include outcomes of income and expense verification or information confirming cash flows and prior rental history that real estate agents require before renting a property to new tenants.[35]

- *Tiering of obligations*:

> The accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging suitable parties from participating in the Consumer Data Right. A tiered, risk-based accreditation model should be used to minimise costs for prospective participants.[36]
> The accreditation criteria must set out any minimum level of insurance coverage required by those eligible for lower tiers of accreditation, to provide assurance that losses from data breaches can be recovered. Allowing lower tiers of accreditation will also provide insurers greater clarity regarding the limitations of various users of the CDR, so insurers can match their coverage to the specific risks faced by an ADR.[37]
> A detailed segregation or delineation of the roles, responsibilities and protections required for each tier will also provide a clear scope for auditors to address when providing assurance services, such as what levels of information security safeguards are applicable.[38]

- *Aligning similar data safety accreditations; recognising external data safety accreditations:* where external data safety accreditations align with Consumer Data Right requirements, these could be recognised in the CDR Regime or at least enable the holders of those external accreditations to go through streamlined CDR accreditation.[39]

What happens next?

I suggest that by no later than 2 years from now (ie by the end of March 2023) Australian FinTechs will have the option of participating in the CDR Regime using the "CDR as a Service" model or a variant of it.

Sponsor's liability for breaches by its affiliates/authorised representatives

For my bold prediction to be fulfilled, one of the key issues to be addressed is the extent of a Sponsor's liability for breaches of the rules of the CDR Regime by affiliates or authorised representatives. Policy makers will need to work with regulators, insurers, the finance industry and consumer advocates to determine the appropriate scope and type of a sponsor's liability in these circumstances.

In addressing the issue as to the liability of sponsors, special rules will most likely need to be made for accounting and business platforms that provide services to businesses as well as accountants and bookkeepers. One major platform contends that once banking data is connected to the general accounting ledger in its system, the data should be considered to be "materially enhanced data" that should therefore no longer be treated as CDR data under the designation relating to the banking sector.[40] Another major platform has expressed concern that data connected to the general accounting ledger may be derived data that is within the CDR Regime despite the fact that the Ministerial designation applies to the banking sector and not the accounting sector.[41] It adds that it is a "digital service provider" which complies with the Australian Taxation Office Security Standard for Add-on Marketplaces (SSAM). It contends that it is not reasonable for digital service providers like it to bear ultimate responsibility for the compliance of its affiliates in the manner that was suggested in the CDR Expansion Consultation Paper. One reason for this is that the platform operates in an ecosystem that is subject to the SSAM.

To the extent that accounting and business platforms dispense with direct bank feeds and become ADRs under the CDR regime, it may be possible for them to be subject to different liability rules in reliance on their affiliates/authorised representatives being accredited under the SSAM. This would be consistent with the recommendation in the CDR Future Directions Report about the recognition of external data safety accreditations.[42]

The difference of approach between prospective intermediaries whose business models involve taking responsibility for their affiliates/authorised representatives[43] and the business and accounting platforms which are resisting taking on liability in this way may be explicable on account of the different contexts in which those two groups operate. I understand that, outside the CDR Regime, the major business and accounting platforms typically obtain Australian bank data by way of direct bank feeds under bilateral arrangements with banks; ie screen scraping accounts for only a small proportion of the bank data that is pulled into those platforms. Further, the platforms often provide their services in a regulated SSAM environment. In contrast, intermediaries which manage ecosystems outside the CDR Regime containing bank data collected via screen scraping may have a relatively higher incentive to police the data security of their ecosystems (including their affiliates' data security) given that screen scraping continues to dwell in an uncertain space from a legal perspective.[44]

Screen scraping

The Australian Securities and Investments Commission's second consultation paper on amendments to the ePayments Code is due to be released shortly. It is not clear if that paper will recommend any changes to the risk allocation between a Code subscriber and its customers for unauthorised transactions where the customer has voluntarily disclosed their login details to a FinTech or an intermediary in a screen scraping process. Several FinTech submissions to the Bragg Committee suggested that the ePayments Code should be amended to specifically allow for screen scraping practices; consumer advocates strongly disagreed with that suggestion.[45] The Bragg Committee's interim recommendation was that:

> ... an outright ban on screen scraping is not prudent at the present time, ... in many cases these practices are enabling companies to innovate and provide competition in the financial services sector. This situation should continue to be monitored, however, as Open Banking is rolled out.[46]

In the specific context of payment initiation only (as opposed to "read only" access or other types of action initiation) the CDR Future Directions Report recommended the eventual prohibition of screen scraping once CDR payment initiation is fully implemented as a viable alternative.[47]

The CDR Regime is in its infancy. As of 6 April 2021, only nine data recipients have been accredited, and only three of those nine are active. Over time, some participants will rely solely on the CDR Regime and others will rely solely on other data capture methods like screen scraping and direct bank feeds. Others will use the CDR and other data capture methods concurrently. This is recognised in the ACCC's Guidance on Screen Scraping released on 26 March 2021[48] which notes that some ADRs may obtain data through both CDR and non-CDR mechanisms. As a result, the guidance states that ADRs need to design their consent flows carefully to ensure that they comply with the CDR Regime and do not mislead consumers. The ACCC's examples of ADR conduct that would be problematic include the following:

- Bundling CDR consents with screen scraping consents.
- Implying that data will be collected through the CDR when screen scraping is actually being used.
- Implying that data collected via screen scraping is subject to the same protection as CDR data.

Conclusion

Enabling FinTechs' cost effective access to the CDR Regime, in conjunction with the continued availability of other data capture options, in a legal and IT environment that appropriately takes account of consumers' safety, privacy and confidentiality, will do much to promote a vigorous and innovative FinTech industry in Australia. I believe this will happen within the next 2 years.

David Kreltszheim
Special Counsel
Cornwalls
d.kreltszheim@cornwalls.com.au
www.cornwalls.com.au

David is a banking, payments, data and regulatory lawyer. His clients include banks and established and emerging Fintechs. The views expressed are the author's and do not necessarily reflect those of Cornwalls.

Footnotes

1. Competition and Consumer Act 2010 (Cth), Pt IVD and the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) (CDR Rules).
2. Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (Cth).
3. See the Australian Competition and Consumer Commission, Consumer date right (CDR) — Project overview, accessed 28 March 2021, www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.
4. See D Kreltszheim "Closing the deal on open banking" (2018) 34(2) *BLB* 28. Also see A Flannery, "Australia's consumer data right is now a reality: implementation in the financial sector" (2019) 35(7) *BLB* 123.
5. FinTech is:

   > . . . the technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. It is an emerging industry that uses technology to improve activities in finance . . . Financial technology companies consist of both startups and established financial institutions and technology companies trying to replace or enhance the usage of financial services provided by existing financial companies.

   See: Wikipedia, Financial Technology, viewed 28 March 2021, https://en.wikipedia.org/wiki/Financial_technology.
6. See FinTech Australia *Submission to the Australian Competition and Consumer Commission: Consumer Data Right — Participation of third party service Providers* (January 2020) p 6, accessed 28 March 2021, www.accc.gov.au/system/files/CDR%20Rules%20-%20Intermediaries%20consultation%20submission%20-%20Fintech%20Australia%20REDACT.pdf; also see Illion (Formerly Dun & Bradstreet), Submission to the ACCC Consultation of the CDR Rules Expansion Amendments, 24 October 2020, p 2, accessed 28 March 2021, available at www.accc.gov.au/system/files/illion%20%2826%20October%202020%29.pdf.
7. See the Australian Senate, *Select Committee on Financial Technology and Regulatory Technology: Interim Report* (September 2020), p 137.
8. Above, pp 142–143.

9. Above n 1, Sch 3.
10. Above n 1, Pt 4, Div 4.3.
11. Above n 1, Pt 4, Div 4.4.
12. In this instance, "privacy" extends to the protection of CDR data that is not "personal information", ie CDR data of consumers who are not natural persons, eg companies and other artificial legal persons.
13. Competition and Consumer Act, above n 1, Pt IVD, Div 5 (privacy safeguards).
14. See Australian Government, *Consumer Data Right Supplementary Accreditation Guidelines: Information Security* Version 2.0 (October 2020), accessed 28 March 2021 www.accc.gov.au/system/files/CDR%20-%20Accreditation%20-%20Supplementary%20Accreditation%20Guidelines%20Information%20Security.pdf.
15. See Australian Government, *Consumer Data Right Rules Expansion Amendments Consultation Paper* (September 2020), accessed 28 March 2021, www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf (CDR Expansion Consultation Paper).
16. See True Layer, *Consultation on Consumer Data Right Rules Updates per September 2020* (October 2020), p 11, accessed viewed on 28 March 2021, www.accc.gov.au/system/files/TrueLayer%20%2829%20October%202020%29.pdf; Envestnet Yodlee, Response to the ACCC Draft Rules that Allow for Accredited Collecting Third Parties (Intermediaries) to Participate in the Consumer Data Right, pp 1–2, accessed 28 March 2021, www.accc.gov.au/system/files/Envestnet%20Yodlee%20%2829%20October%202020%29.pdf.
17. See text associated with nn 30 to 39 below.
18. Contra True Layer, above n 16, suggesting that the affiliate (B) should not need to be accredited in its own right.
19. The CDR Expansion Consultation Paper, above n 15, at p 16, suggests that there be an annual attestation by the sponsor A that its affiliate B continues to meet the accreditation criteria, including evidence of an annual self-assessment and attestation statement by B regarding its continued compliance with Sch 2 of the CDR Rules, above n 1.
20. See Envestnet Yodlee, above n 16, p 4.
21. Above n 15, p 15.
22. Above n 15, p 9.
23. Above n 15, pp 11–12.
24. Above n 15, pp 13–15.
25. Above n 15, pp 15–17.
26. See ACCC, Consumer data right — Submissions, accessed 28 March 2021 www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-consumer-data-right-rules.
27. See Office of the Australian Information Commissioner, OAIC Submission to the CDR Rules Expansion Amendments Consultation" (29 October 2020), p 3; Office of the Victorian Information Commissioner, *Submission in response to the Consultation Paper on CDR Rules Expansion* (29 October 2020); FinTech Australia, *Submission to the Australian Competition and Consumer Commission Consumer Data Right — Consultation on proposed changes to the CDR Rules* (November 2020), p 5; Australian Banking Association, *ACCC Consultation on Proposed Changes to the CDR Rules* (29 October 2020) pp 1, 4. All these submissions are available at the link specified above n 26.
28. See the True Layer and Envestnet Yodlee submissions, above n 16.
29. See Xero, *Consultation on Proposed Changes to the CDR Rules* (5 November 2020) pp 3–4, accessed 28 March 2021, www.accc.gov.au/system/files/Xero%20%285%20November%202020%29.pdf.
30. See Australian Government, *Future Directions for the Consumer Data Right* (October 2020, publicly released on 23 December 2020).
31. Above, at p 109 (Recommendation 6.4).
32. Above n 30, at p 112 (Recommendation 6.6); *Select Committee on Financial Technology and Regulatory Technology: Interim Report,* above n 7.
33. Above n 30, at pp 110–112.
34. Above n 30, at pp 112–113 (Recommendation 6.8).
35. Above.
36. Above n 30, at p 119 (Recommendation 6.12).
37. Above.
38. Above.
39. Above n 30, at pp 194–195 (Recommendations 8.6 and 8.7).
40. See MYOB, "Submission to Senate Select Committee on Financial Technology and Regulatory Technology" (December 2020), at p 7. The Ministerial designation is set out in the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation, above n 2. Sections 5(1)(b) and 9 of that designation exclude "materially enhanced information" from the ambit of the data that is covered by that designation.
41. See Xero, above n 29, pp 1–2.
42. See n 39 above and the associated text.
43. See the submissions referenced at n 16 above.
44. See D Kreltszheim, above n 4, p 30.
45. See above n 7, pp 149–150.
46. See above n 7, p 220.
47. See above n 30, at p 97.
48. See ACCC, Guidance on Screen Scraping (26 March 2021), accessed 28 March 2021, https://cdr-support.zendesk.com/hc/en-us/articles/900005316646-Guidance-on-screen-scraping.

Australian
Banking & Finance
Law Bulletin

For editorial enquiries and unsolicited article proposals please contact newsletters@lexisnexis.com.au.
Cite this issue as (2021) 37(2) *BLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1035-2155 Print Post Approved PP 255003/00764