COVERSHEET

Minister	Hon Dr David Clark	**Portfolio**	Commerce and Consumer Affairs
Title of Cabinet paper	Further decisions on the consumer data right	**Date to be published**	19 December 2022

List of documents that have been proactively released		
Date	**Title**	**Author**
27 July 2022	Further decisions on the consumer data right	Office of the Minister of Commerce and Consumer Affairs
27 July 2022	DEV-22-MIN-0151 - Consumer Data Right: Further Decisions	Cabinet Office
15 March 2022	2122-2226 - Updated Consumer Data Right	MBIE
July 2022	Supplementary Regulatory Impact Statement: Further decisions on establishing a consumer data right	MBIE

Information redacted **YES**

Any information redacted in this document is redacted in accordance with MBIE's policy on Proactive Release and is labelled with the reason for redaction. This may include information that would be redacted if this information was requested under Official Information Act 1982. Where this is the case, the reasons for withholding information are listed below. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

© Crown Copyright, Creative Commons Attribution 4.0 International (CC BY 4.0)

BRIEFING

Updated Consumer Data Right

Date:	15 March 2022	**Priority:**	Medium
Security classification:	**In Confidence**	**Tracking number:**	2122-2226

Action sought		
	Action sought	**Deadline**
Hon Dr David Clark Minister of Commerce and Consumer Affairs	**Agree** to provide officials with feedback on further advice on the institutional arrangements and the liability and penalties regime for the consumer data right.	22 March 2022

Contact for telephone discussion (if required)				
Name	**Position**	**Telephone**		**1st contact**
Glen Hildreth	Acting Manager, Competition and Consumer Policy	Privacy of natural persons		
Yi-Shen Lau	Senior Policy Advisor			✓
Clark Samuel	Graduate Policy Advisor			

The following departments/agencies have been consulted:
Commerce Commission, Public Service Commission.

Minister's office to complete:

☐ Approved ☐ Declined
☐ Noted ☐ Needs change
☐ Seen ☐ Overtaken by Events
☐ See Minister's Notes ☐ Withdrawn

Comments:

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

BRIEFING

Updated Consumer Data Right

Date:	15 March 2022	**Priority:**	Medium
Security classification:	**In Confidence**	**Tracking number:**	2122-2226

Purpose

To advise you on the remaining policy decisions for the drafting of a Consumer Data Right Bill. These decisions relate to the appropriate agency for certain institutional responsibilities and the liability and penalties regime.

Executive summary

1. Cabinet has agreed to establish a consumer data right (CDR) legislative framework, and has made high-level policy decisions for that framework [DEV-12-MIN-0145]. Cabinet invited you to report back by 30 November 2021 (later extended to early 2022) on institutional arrangements, cost recovery, compliance, enforcement and consumer redress for the CDR, and noted that it would further consider funding implications at the same time.

2. We previously advised you on these matters. You asked for further advice on institutional arrangements and penalties.

Institutional arrangements

3. We do not yet have a complete view of the costs, risks and benefits of the Commerce Commission taking on the enforcement function. We are carrying further work on this, which is likely to involve getting external actuarial and/or technical advice.

4. To avoid delays, we propose that the exposure draft be used to seek feedback on the appropriate enforcement agency. Commerce Commission staff have raised concerns about being named as the regulator in the exposure draft, so we propose that the exposure draft simply refer to a "[department or Crown entity]" or similar.

5. Regardless of who carries out the enforcement function, we consider that there is sufficient rationale for keeping the policy and service delivery functions together in a department, and also recommend that the data standards should be made by a statutory officer within the administering department."

Pecuniary penalties

6. Pecuniary penalties should apply to a range of CDR breaches for which infringement offences are insufficient or criminal proceedings too heavy handed.

Custodial sentences

7. We have given further consideration to whether custodial sentences should apply. The relevant factors are the seriousness of the offences, proportionality, and the principle of least criminality.

8. Based on those factors, custodial sentences are not appropriate for the majority of offences in the CDR regime. However, they are appropriate for the worst cases of criminal offending, such as in cases where a person obtains, or causes loss by:

a. knowingly misleading or deceiving another person into believing that someone is a CDR consumer or a person making a valid request or consent for the disclosure of CDR data

b. fraudulently holding out that they are an accredited person (or a particular type/level of accredited person).

9. Although custodial sentences may be available in a statute, the decision whether to impose a custodial sentence is ultimately made by the courts on the facts of each case.

Next steps

10. Following your feedback on this briefing, we will provide you with an updated Cabinet paper, covering institutional arrangements, cost recovery, compliance/ enforcement, consumer redress, and banking as the first designation to be considered. We anticipate that you will take this paper to DEV in April.

Confidential advice to Government

Recommended action

The Ministry of Business, Innovation and Employment recommends that you:

a **Note** that Cabinet agreed to develop a consumer data right in June 2021, and that you requested further advice regarding the institutional arrangements and penalties.

Noted

Institutional arrangements

b **Agree** to the policy and service delivery functions remaining together in the administering department for CDR, regardless of where the enforcement function is located.

Agree / Disagree

c **Note** that officials have not been able to come to a complete view of the costs, risks and benefits of the Commerce Commission taking on the enforcement function.

Noted

d **Agree** that the exposure draft will seek feedback on the suitable entity to carry out the enforcement function.

Agree / Disagree

e **Agree** that the exposure draft provide for a statutory officer within the administering department, who is responsible for making data standards.

Agree / Disagree

Penalties

f **Note** that you previously agreed that:

- **a.** criminal offences would apply to prohibited conduct that involves serious harm and/or is morally blameworthy, such as instances of fraud and deceptive or misleading conduct, and
- **b.** pecuniary penalties would apply to prohibited conduct where a criminal conviction is inappropriate and a monetary penalty sufficient to deter or punish breaches.

Noted

g **Note** that pecuniary penalties are likely to be the suitable penalty for some prohibited conduct within the CDR regime.

Noted

h **Agree** that custodial sentences should be an available penalty for the most serious criminal offences in the CDR Bill, such as instances where a person obtains, or causes loss by means of fraud and certain deceptive or misleading conduct.

Agree / Disagree

i **Note** that officials will provide you a list of proposed penalty tiers for the different offences with the updated Cabinet paper.

Noted

Next steps

j **Note** that, following your feedback, we will provide you with a Cabinet paper covering institutional arrangements, cost recovery, compliance/enforcement, consumer redress, and banking as the first designation to be considered) for DEV in April.

Noted

Confidential advice to Government

l **Agree** to officials seeking from the Cabinet Office an extension of timeframe for reporting back on most matters of the CDR Bill to May 2022.

Agree / Disagree

Agree / Disagree

Glen Hildreth
Acting Manager, Competition and Consumer Policy

15 / 03 / 2022

Hon Dr David Clark
Minister of Commerce and Consumer Affairs

..... / ...... / ......

Background

1. On 30 June 2021, Cabinet Economic Development Committee (DEV) agreed to establish a consumer data right (CDR) legislative framework [DEV-12-MIN-0145].

2. Cabinet agreed that the consumer data right will require businesses that hold data (data holders) to share prescribed data that they hold about consumers (CDR data) with trusted third parties (accredited persons, or data recipients), on the consent of the consumer. The consumer data right will be applied to a certain sector, industry or market, and to certain data sets, via an Order in Council.

3. In September and December 2021, we provided you with further advice on remaining policy decisions for the CDR Bill [briefings 2122-0852 and 2122-1984 refers]. Officials made recommendations on institutional responsibilities (i.e. which entities should be allocated what functions), cost recovery, compliance and enforcement, and consumer redress.

4. You agreed to the following recommendations:

   a. That MBIE be responsible for advising on secondary legislation (regulations and sector designations.

   b. That data standards be determined on a sector-by-sector basis, with a data standards body within MBIE as the backstop. The process would provide for wider input at a technical and sector level.

   c. In relation to liability and penalties, that:

      i. Penalties for breaches would include a combination of criminal offences, pecuniary penalties and infringement offences

      ii. Criminal offences should apply to prohibited conduct that involves serious or significant harm and/or is morally blameworthy.

      iii. Pecuniary penalties should apply if the offending does not warrant the denunciatory and stigmatising effects of a criminal conviction and a monetary penalty would be sufficient to deter or punish breaches

      iv. Relatively minor breaches of the CDR requirements can be treated as infringement offences

   d. that the CDR Bill would provide for fees and for levies to be prescribed in regulations

   e. that the Cabinet paper would seek agreement for banking to be the first sector considered for designation.

5. You agreed to maximum penalties for criminal offences, pecuniary penalties and infringement offences. You also agreed to two cases in which criminal offences would apply.

6. You asked for further advice on the institutional arrangements and enforcement regime for the CDR. This briefing provides you with some of that requested advice, ahead of providing you with an updated Cabinet paper and further accompanying briefing.

Institutional arrangements

Introduction

7. This section of the briefing advises you on the agencies that should be responsible for the CDR functions. To recap, the functions are as follows:

Type of function	Specific CDR functions
Policy (*making the rules*)	• Advice on CDR Act and regulations/CDR rules (high level and moderately detailed policy) • Creation of data standards (very detailed policy)
Service delivery (*implementing the rules*)	• Accrediting data recipients • Providing the registry • Promoting the CDR regime
Enforcement (*making sure the rules are followed*)	• Monitoring and compliance
Dispute resolution (*making things right for consumers*)	• Consumer dispute resolution

8. We previously recommended that MBIE be responsible for the policy, service delivery, and enforcement functions, with the Privacy Commissioner responsible for the dispute resolution function for individuals [briefing 2122-1984 refers]. This was based on our framework for decision-making about the CDR institutional responsibilities, which included consideration of the following factors:

   a. That functions should sit with a department unless good reasons exist to do otherwise.

   b. In choosing a specific body to carry out a function, relevant factors to consider include, fit with existing functions, competency, cost, and promoting trust and confidence.

   c. The legislative regime should be designed flexibly.

9. You previously agreed that advice on the Act and regulations be made by MBIE [briefing 2122-1984]. We note that the usual drafting approach for assigning functions is to assign them to the "administering department" to be decided later by the Prime Minister's office. This gives a measure of flexibility, though in practice the likely options would be MBIE or DIA. Accordingly, this briefing refers to various functions being assigned to an "administering department", not "MBIE", given that this will be the wording in the Bill.

10. You requested further advice on the other functions and asked officials to investigate whether the Commerce Commission could carry out the enforcement function.

Policy and service delivery functions should stay together in administering department

11. We have reconsidered the approach to the institutional arrangements. We recommend that the policy and service delivery functions stay together in the administering department, regardless of where the compliance function sits:

Policy (*making the rules*)	• Advice on CDR Act and regulations/CDR rules (high level and moderately detailed policy) • Creation of data standards (very detailed policy)
Service delivery (*implementing the rules*)	• Accrediting data recipients • Providing the registry • Promoting the CDR regime

Policy functions should be carried out by the administering department

12. As discussed earlier, you agreed that the advice on the Act and regulations be given by the administering department. This is appropriate given that Cabinet and Ministers will be making decisions on the Act and regulations.

13. We recommend that the other policy function – data standards – also be carried out by the administering department. This would create good continuity between the Act and regulations (high-level and moderately detailed policy) and the creation of data standards (very detailed policy). We are aware from Australia that having multiple entities involved in these different functions has caused confusion. Australia initially assigned the data standards function to their Commonwealth Scientific and Industrial Research Organisation but has since moved that function to Treasury (which carries out the other policy functions as well).

14. We advise you further on the data standards function later in this briefing.

Policy and service delivery functions should stay together

15. We recommend that the policy and service delivery functions be located in the same administering department. We do not recommend that they be split, even if the enforcement function is carried out by a different department or Crown entity, such as the Commerce Commission.

16. The implementation of the CDR regime will be technology-focussed and will involve an IT build. By way of comparison, the Australian Competition and Consumer Commission (ACCC) has advised that two thirds of the cost of their regime so far have been for developing technology-related elements such as:

    a. Developing the data standards, which set out the technical requirements for participants (for example, in relation to information security, form of data, interface between participants, and customer experience).

    b. The registry, which ensures security and privacy for CDR transactions behind the scenes by providing a system for participants to verify the person to whom they are sending information is necessary. In Australia, accredited participants get an encryption key through the register that identifies their computers as accredited. Before every data transaction, the data holder's computer contacts the register to make sure the computer receiving the information belongs to an accredited person. The actual transfer of data then occurs bilaterally.

    c. Accreditation platforms and systems, and potentially staff to assess technical elements of applications for accreditation.

    d. Technical assistance for participants to engage with accreditation and the register (part of the promotion and education function).

17. In many policy areas, it is appropriate for policy and service delivery elements to be carried out by different agencies, as there is little overlap between the skills required for each and few synergies between the two. CDR is different because it is oriented towards building and regulating data and information systems. As a result, parts of the policy are extremely detailed, and much of the success will lie in the way that the whole system functions as a whole. It will be critical to the success of the regime that the policy and service delivery teams collaborate closely together to ensure that the system works from a technical and customer experience perspective. That way, standards can be closely aligned with the specialist technology teams that are designing, building, and operating the regime's infrastructure build. This can best be achieved if the teams are in the same department.

18. Staff at the ACCC highlighted to us that there are considerable synergies between the policy and service delivery functions. Failing to realise these synergies increases the risk of a lower-quality end product and will add costs to the regime.

19. Having these functions in the same department will also be simpler for CDR participants, giving them a single point of contact when they get accredited and begin to participate in the regime. We understand that this is one of the primary criticisms of the early stages of the CDR in Australia.

20. For completeness, the registry and accreditation functions are carried out by the ACCC in Australia. They are not carried out by the policy agency (Australian Treasury). This may reflect the fact that the Australian Treasury has very little service delivery capability or experience. In contrast, Government departments including MBIE and DIA have considerable service delivery capability and experience.

Advice on the Commerce Commission being the agency responsible for enforcement

21. We have given further consideration as to which entity should be responsible for the enforcement of CDR, and in doing so have had discussions with officials at the Commerce Commission and the Public Service Commission.

22. We have not been able to come to a view on the costs, risks and benefits of the Commerce Commission carrying out the enforcement function.

23. We are carrying out further work to determine the cost and resource implications of the CDR, including the different options for the institutional arrangements. This is likely to involve getting external actuarial and technology/IT advice as appropriate to help assess the cost of implementing various aspects of the CDR regime.

We propose to seek feedback on the enforcement agency in the exposure draft

24. In the interests of timing, we propose that the exposure draft is used to seek feedback on the agency responsible for enforcement. This will allow us to progress the drafting process while we get more information on the likely cost implications of the CDR regime.

25. Commerce Commission staff have raised concerns about being named as the regulator in the exposure draft. We therefore propose that the exposure draft simply refer to a "[department or Crown entity]" or similar. We will seek advice on the correct approach from PCO during the drafting process.

Data standards function should be a centralised statutory officer within administering department

26. We previously recommended that the institutional arrangements for data standards be determined on a sector-by-sector basis, with a data standards body within MBIE as a backstop.

27. We have further considered how the data standards function could work, including consulting with the Chair of the Data Standards Body in Australia. As a result of that, we now consider a sector-by-sector arrangement unsuitable for the following reasons:

    a. While some of the data standards will be sector specific (for example, technical rules about the form of data), other data standards will be the same across sectors (including information security, customer experience, many standards relating to how participants interact with each other in the CDR ecosystem ("endpoints").

    b. A sector-specific approach would make interoperability more difficult, especially as the CDR regime gets bigger. Data may not be able to be shared across sectors if the data standards are different for each sector.

    c. Given how technical the data standards are, it will be important for the regulations, data standards, accreditation systems and registry to be developed in close collaboration

(as previously discussed). This will be more difficult if the data standards are developed in each sector.

28. Instead, we recommend that the exposure draft provide for a statutory officer within the administering department, who is responsible for making data standards. This is the same arrangement as Australia, whose Chair of the Data Standards Body is a statutory officer. The creation of a statutory officer would safeguard the function. It would also enable it to move to different agencies over time, should that be needed.

29. We anticipate that the standards themselves would be developed by a data standards team within the administering department. Any standards developed by industry could be adopted into this development process, as appropriate, in consultation with the industry.

30. We will get further clarity on the arrangements as we move through the drafting and exposure draft process, but we anticipate that the process could look like this:

Liabilities and penalties regime for breaches of the consumer data right regime

Background

31. You have requested further advice on pecuniary penalties and custodial sentences.

32. You previously agreed that breaches of CDR requirements could result in infringement offences, pecuniary penalties or criminal offences, depending on the nature of the breach [briefing 2122-1984 refers]. You also agreed on maximum penalties for each, as well as the broad circumstances in which each type of sanction would apply.

33. To recap, Table 1 below outlines the key features of each type of sanction and when they might be used.

Table 1

Category of sanction	Results in conviction?	Consequences for breach	When the category should be used
Criminal offence – criminal sanction Offences proved beyond reasonable doubt.	Yes. This has serious consequences for the individual e.g. stigma, future employment and travel.	Criminal conviction. Monetary penalty or imprisonment.	Egregious contraventions of CDR law, involving significant harm to the individual or public interest. The behaviour must be reckless or intentional. A CDR example would be a person fraudulently holding out that they are an accredited person (or a particular type/level of accredited person) to access private information for pecuniary gain
Pecuniary penalty – civil sanction Breaches proved 'on the balance of probabilities.	No	Monetary penalty. Breaches are usually made public, which has reputational consequences.	Broad civil liability for behaviour beyond basic contraventions, but not so sufficiently egregious to warrant the use of serious criminal offences. This category will be important for deterrence and will also provide a mechanism for wronged participants of a CDR regime to seek compensation. Penalty would be monetary.
Infringement offence – minor criminal sanction. Offences proved on strict or absolute liability	No	Infringement notices. Minor fines.	Minor contravention of the law. Contraventions with basic 'compliance' obligations that would not have serious consequences Would be used for behaviour that results in simple clear-cut contraventions of the law.

			A CDR example would be an accredited data recipient (a Fintech) failing to accurately record a consumers' consent for the purpose of making a consumer data request.

34. These offences and penalties would complement the licensing regime and other regulatory tools. For example, the accreditation agency would have the ability to revoke or suspend accreditations, which will incentivise compliance by data recipients. Removing non-compliant participants from the CDR regime is a powerful tool that the accreditation agency can wield to curb repeated or serious offending and safeguard a designated sector.

Further advice on pecuniary penalties

35. You have previously agreed to the inclusion of pecuniary penalties for the CDR regime.

36. Pecuniary penalties are a valid tool for regulatory enforcement, providing an intermediate penalty between criminal and infringement offences. We consider that pecuniary penalties will provide adequate deterrence for breaches for which infringement offences are insufficient or criminal proceedings too heavy handed.

37. This follows the rationale that for commercial misconduct, enforcement is best dealt with through the civil law unless the conduct sufficiently warrants the intervention of criminal sanctions.

38. Some examples of offending that we envisage would be subject to pecuniary penalties include:

    a. a data holder refuses to provide CDR services to consumers or data recipients in defiance of, or not in accordance with, a CDR designation

    b. a data holder fails to authenticate the identity of a person requesting the consumer data, as required under the consumer data rules, which then results in a customer's data being transferred without their consent

    c. a data holder fails to authenticate the identity of a third party requesting a consumer's data, as required under the consumer data rules, which then results in the data holder sending their customer's data to a third party that is not an approved data recipient

    d. a data recipient fails to adequately safeguard CDR data they receive, as required under the consumer data rules, or a data breach occurs during the transfer of CDR data, which then results in a financial loss to the consumer.

39. The Legislation Design Advisory Committee Guidelines (2021) note the following: "Compelling reasons must exist to justify applying the criminal law to conduct. Depending on the seriousness of the misconduct, a person subject to a criminal conviction may experience a loss of liberty (imprisonment or home detention), a loss of property (confiscation, fines, or reparation), or both. A person who is convicted acquires the stigma of a criminal conviction, which may affect future employment or overseas travel".

40. The types of breaches listed above do not warrant the denunciatory and stigmatising effects of a criminal conviction (e.g., the conduct does not have an element of intent, dishonesty or recklessness, having regard to the harm that may be caused). In light of this we consider pecuniary penalties may be more appropriate in deterring and punishing corporate offenders. Pecuniary penalties are imposed under civil law. While they may involve very large sums of money, neither imprisonment nor criminal conviction can result.

41. This approach is consistent with the Australian approach, which provides for pecuniary penalties (in addition to criminal offences and infringement offences).

Next steps

42. We previously provided you with advice on maximum penalties for criminal offences, pecuniary penalties and infringement offences. Officials are preparing a more detailed list of penalty tiers for the CDR regime to ensure that penalties are proportionate. We will provide you with this list with the updated Cabinet paper. As part of that process, we will consult with the Ministry of Justice.

We recommend that custodial sentences for serious criminal offences in the primary CDR legislation

Background

43. We previously recommended that custodial sentences should not be available for offences in the CDR Bill. The primary reasons for this advice were:

    a. to avoid a chilling effect on participation in the CDR regime and,

    b. because custodial sentences were already available under the Crimes Act (for example, for section 240 of the Act, which relates to knowingly, recklessly or intentionally obtaining by deception or causing loss by deception).

44. We have given further consideration to this issue. For the reasons set out in this section of the briefing, we now recommend that the CDR penalty regime would be best served by including custodial sentences within the primary legislation for the most egregious offences under the CDR.

Relevant considerations when considering the appropriateness of custodial sentences

45. Based on advice from the Ministry of Justice and LDAC's *Legislation Guidelines*, we consider that the relevant considerations when considering the appropriateness of custodial sentences are:

    a. The **seriousness of the conduct**. The factors from the *Legislation Guidelines* that are most relevant in the CDR context are:

        i. Whether the conduct involves fraud, bribery or corruption

        ii. Whether the conduct is morally blameworthy, having regard to the required intent and the harm that may result

        iii. Whether the harm that would result from the conduct is foreseeable and avoidable by the offender (e.g., it involves an element of intent, premeditation, dishonesty, or recklessness in the knowledge that the harms may eventuate).

    b. The **punishment is proportionate to the prohibited conduct**. Imposing criminal and custodial sanctions is a serious matter that has significant consequences for convicted individuals.

    c. The principle of **least criminality**. That is, penalties should be set at the lowest point possible that still achieves the desired objectives. In relation to this, recent academic thinking is that the likelihood of getting caught is a stronger deterrent than a high penalty.

Custodial sentences would be appropriate for the worst cases of possible offending

46. Based on the above factors, custodial sentences are not appropriate for the majority of criminal offences. The harm for most of the breaches is a breach of privacy, which is not the kind of harm that usually warrants a term of imprisonment.

47. However, custodial sentences would be proportionate for a very limited number of situations that reflect the worst cases of possible offending, such as some cases in which a person obtains, or causes loss by:

    c. knowingly misleading or deceiving another person into believing that someone is a CDR consumer or a person making a valid request or consent for the disclosure of CDR data

    d. fraudulently holding out that they are an accredited person (or a particular type/level of accredited person).

48. Furthermore, although custodial sentences may be available in a statute, the decision as to precisely what penalty will be imposed in a particular case belong entirely with the courts. When imposing a sentence, the courts have regard to the maximum penalty available, the particular facts of the case, the guidance and principles set out in the Sentencing Act 2002, and guidance in legislation and from the higher courts.

Custodial sentences would be consistent with the approach in Australia and in comparable NZ legislation

49. Custodial sentences would be consistent with the approach in Australia for CDR. For example, the Australian legislation provides for up to 5 years imprisonment for persons engaged in misleading or deceptive conduct in relation to CDR data.

50. Custodial sentences would also be consistent with the approach in comparable New Zealand legislation including the New Zealand Commerce Act 1986, Credit Contracts and Consumer Finance Act 2003 and Financial Markets Conduct Act 2013.

51. More detail on the penalties in the Australian CDR regime and comparable New Zealand legislation is included in Annex 1.

We do not think custodial sentences will significantly deter participation in the regime

52. One reason we initially recommended against custodial sentences was to avoid a chilling effect. The concern was that including custodial sentences within the CDR regime may discourage businesses from participating in the CDR, reducing the expected benefits from the CDR regime.

53. However, custodial sentences are being proposed only for the very worst offending where a person has deliberately misled customers for financial gain, and has the potential to jeopardise the integrity of the CDR. Even when a custodial sentence is an available penalty, it would be up to the court to decide whether a custodial sentence is warranted in a particular case. Given that, along with the fact that broader senses of these egregious offences already exist in legislation such as the Crimes Act, we do not think there will be a significant chilling effect to impose custodial sentences for those offences.

54. We do acknowledge there is a trade-off between designing a regime that encourages participation (with the associated scale benefits that come from reaching critical mass) versus ensuring confidence in the security and integrity of the regime through the provisions of offences and penalties, including custodial sentences. The majority of the CDR offences will not carry custodial sentences and as such we consider that the inclusion of custodial sentences strikes the right balance.

CDR-specific custodial sentences will be more transparent and clearer for CDR participants

55. Having CDR-specific offences will make enforcement more transparent for participants. The potential consequences for participants if they commit certain egregious offences will be clearer if they are included in the CDR Bill.

56. It will also be clear that the CDR enforcement agency is responsible for those offences, reducing the risk of "enforcement gaps" forming due to multiple agencies being responsible for enforcement of offences under the Crimes Act. Having multiple agencies responsible for enforcement and compliance can sometimes lead to sub-optimal outcomes and undermine confidence in the system.

Next steps

57. Please provide us with your feedback on the above advice. We will then provide you with an updated Cabinet paper reflecting that feedback. As part of preparing that Cabinet paper, we will consult further with the Ministry of Justice.

58. As discussed earlier in this paper, officials are preparing a more detailed list of penalty tiers, which will include the offences that warrant custodial sentences. Advice on this will accompany the updated Cabinet paper.

Consultation

59. In developing the advice for this briefing, we have consulted with a range of government agencies including the Ministry of Justice, the Commerce Commission, the Public Service Commission, Office of the Privacy Commissioner, and Inland Revenue.

60. We also met with a range of Australian government agencies including the Chair of the Data Standards Body, the Australian Treasury, and the ACCC.

61. We also consulted with Scott Farrell, who led the Australian Government's Open Banking Inquiry and the Inquiry into Future Directions for the Consumer Data Right.

Communications and risks

62. We do not anticipate that public communications are suitable at this time.

63. Recently many stakeholders have been interested in the progress of the CDR Bill and have asked for the opportunity to provide feedback. The exposure draft will be the next opportunity for interested parties to engage in the policy process. If stakeholders contact to your office in the meantime, we suggest alerting them to this. Additionally, decisions on CDR will be made public on MBIE's website after they have been passed by Cabinet.

64. In regard to penalties, providing custodial sentences for commercial legislation is often criticised as creating disincentives for business activity. There is also the chance it may negatively influence the regime's uptake, and FinTechs may be discouraged from participating if they are concerned. However, as custodial sentences will only apply to the most serious, unconscionable offences, we believe this risk is small.

Confidential advice to Government

Timing and next steps

Implications for Cabinet report-back timings

66. As noted earlier in this briefing, officials are carrying out further work to determine the cost and resource implications of implementing CDR, including the different options for the institutional arrangements. This has implications for Cabinet report-back timings.

Next steps

70. It is important that we continue to make progress on the drafting process. If the Bill is not introduced this year, this places considerable stress on the timeline for passing the Bill in this parliamentary term.

71. We anticipate the following next steps:

- You provide feedback on this briefing, to be included in an updated Cabinet paper – 22 March 2022
- Cabinet paper lodged for DEV – 28 April 2022
- DEV approves the next round of policy decisions – 4 May 2022
- Exposure draft CDR Bill for public release – Confidential advice to Government
- Cabinet paper with report back on exposure draft changes Confidential advice to Government
- Introduction of the CDR Bill – Confidential advice to Government

Annexes

Annex 1: Custodial sentences in the Australian CDR regime and various New Zealand competition and consumer protection laws.

Annex 1: Custodial sentences in the Australian CDR regime and various New Zealand competition and consumer protection laws

Statute	Type of misconduct / breach	Maximum penalty available (actual can be less)
Australian CDR ***(Criminal offences)***	• Deliberate misleading or deceptive conduct: ➢ There is a specific offence for fraudulent conduct where a person misleads or deceives another person, or is likely to mislead or deceive another person, into believing that: (a) a person is a CDR consumer for CDR data; or (b) a person is making a valid request or consent, or has satisfied other criteria, for the disclosure of CDR data under the consumer data rules (section 56BN) • Holding out that a person is an accredited person. It is a criminal offence if a person fraudulently holds out that the person is an accredited person, an accredited person holding an accreditation granted at a particular level, or an accredited data recipient of CDR data (section 56CC)	The penalty on conviction for a body corporate can be up to the greater of **A$10 million**, **3 times the total value of any benefit accruing** as a result of an offence if the Court can determine the value, or if the value of any benefit accruing cannot be determined by the Court, **10% of the body corporate's annual turnover** during the 12-month period at the end of the month in which an offence happened or began. In the case of an individual, the penalty on conviction can be **imprisonment** for up to **5 years**, a fine of up to **A$500,000**, or both (see sections 56BN and 56CC).
Commerce Act ***(Criminal offences)***	• Entering into or giving effect to a cartel provision (section 30)	**Imprisonment** for up to **7 years** or a fine of **$500,000**, or both, in the case of an individual or in any other case, the greater of **$10million** or either: • if it can be readily ascertained and if the court is satisfied that the offence occurred in the course of producing a commercial gain, **three times the value of any commercial gain** resulting from the contravention, or • if the commercial gain cannot be readily ascertained, **10% of the turnover** of the person and all its interconnected bodies corporate (if any) in each accounting period in which the contravention occurred.
	• Breach of management banning order as a result of entering into or giving effect to the cartel provision in breach of section 30 (section 80C)	**Imprisonment** for up to **5 years** or a fine of **$200,000**.
Fair Trading Act *(Criminal offences)*	•	There are no custodial sentences in the Fair Trading Act. The Commerce Commission can, however, elect to file charges under section 240 of the Crimes Act 1961 where a person knowingly, recklessly or intentional obtains by 'deception' or causes loss by deception (including by making false representations). A person found guilty under section 240 may face **imprisonment** for up to **3 years**.

Statute	Type of misconduct / breach	Maximum penalty available (actual can be less)
CCCF Act ***(Criminal offences)***	• Breach by transferee: in relation to a buy-back transaction; or of a prohibition on dealing with land without leave of the court if initial disclosure has not been made or if no independent legal advice. • A buy-back transaction is where a homeowner transfers their home (or an interest in their home) to a transferee, who typically pays their debts or gives them money. The former homeowner has the right to continue living in the home and to buy it back at some time in the future.	In the case of an individual, **imprisonment** for up to **1 year** or a **$200,000** fine, or both; and in any other case, a **$600,000** fine.
	• Breach of a District Court order not to act as creditor, lessor, transferees or buy-back promoter.	In the case of an individual, **imprisonment** for up to **3 months** or a **$200,000** fine, or both; or in any other case, a **$600,000** fine.
FMC Act ***(Criminal offences)***[1]	• Disclosure of offers of financial products (Part 3) ➢ Under section 48, a person must not make a regulated offer, or distribute an application form for a regulated offer, unless the issuer has o prepared a product disclosure statement for the offer o lodged the product disclosure statement with the Registrar, and o supplied to the Registrar all of the information that the register entry (if any) is required to contain by the FMC Act or the regulations. ➢ Under section 50, a product disclosure statement must be given if an offer requires disclosure. A person who breaches the above requirements commits an offence if the person **knows** that, or is **reckless** as to whether, the offer is a regulated offer.	In the case of an individual, **imprisonment** for up to **5 years**, a fine of **$500,000**, or both; and in any other case, **$2.5 million**.
	• Disclosure of offers of financial products (Part 3) ➢ Under section 88, a person must not offer financial products of an entity that has not been formed or does not exist if the offer would be a regulated offer if the entity did exist.	In the case of an individual, **imprisonment** for up to **3 years**, a fine of **$200,000**, or both; and in any other case, **$600,000**.
	• Dealing in financial products on markets (Part 5) ➢ Section 244 provides for **knowingly** breaching insider conduct provisions ➢ Section 262 prohibits market manipulation through false or misleading statement or information.	In the case of an individual, **imprisonment** for up to **5 years**, a fine of **$500,000**, or both; and in any other case, **$2.5 million**.
	• Financial reporting (Part 7) ➢ Under section 461I, it is an offence to **knowingly** fail to comply with financial reporting standards.	In the case of an individual, **imprisonment** for up to **5 years**, a fine of **$500,000**, or both; and in any other case, **$2.5 million**.

[1] In addition, the Financial Markets Authority Act 2013 empowers the FMA to file charges for offences under certain sections of the Crimes Act 1961. This includes offences of dishonestly taking or using a document (section 228) and obtaining by deception/causing loss by deception (section 240).

Statute	Type of misconduct / breach	Maximum penalty available (actual can be less)
	• Enforcement, liability, and appeals – defective disclosure and false statements (Part 8) ➢ **Knowingly** or **recklessly** breaching prohibition on offers where there is defective disclosure in product disclosure statement or register entry (section 510) ➢ **Knowingly** or **recklessly** breaching prohibitions relating to defective disclosure ➢ Making, or authorising the making of, a statement in it that is false or misleading in a material particular knowing it to be false or misleading ➢ Breaching a banning order made by the High Court ➢ Refusing or failing, without reasonable excuse, to comply with an order made by the FMA.	Maximum penalties in order of the misconduct / breach shown in the second column: • In the case of an individual, **imprisonment** for a term of **10 years**, a fine of **$1 million**, or both and in any other case, a fine of **$5 million** • In the case of an individual, **imprisonment** for a term of **5 years**, a fine of **$500,000**, or both and in any other case, a fine of **$2.5 million** • **Imprisonment** for a term of **5 years**, a fine of **$200,000**, or both • **Imprisonment** for a term of **3 years**, a fine of **$200,000**, or both • A fine of **$300,000**.