Australian Banking Association

27 November 2019

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

Via email: consultation@oaic.gov.au

Dear Shona,

Draft Consumer Data Right Privacy Safeguard Guidelines Consultation

The Australian Banking Association (**ABA**) welcomes the opportunity to make this submission on the Office of the Australian Information Commissioner (**OAIC**) Draft Consumer Data Right Privacy Safeguard Guidelines.

With the active participation of its member banks, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA also works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and community. It strives to ensure Australia's bank customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA appreciates that the draft Privacy Safeguard Guidelines (**PS GL**) are intended to simplify the complex legislative requirements in the Consumer Data Right (**CDR**) regime, whilst taking into account collectively the Consumer Data Rules, Customer Experience Guidelines and the data standards

This ABA submission is in two parts. Part One (Key issues) discusses key issues which relate to complaints, grounds for refusals of request for data, and the potential risks of having both the Privacy Safeguards and Australian Privacy Principles (**APPs**) operating simultaneously. Part two (Targeted feedback) raises concerns of a more detailed nature and references the relevant paragraphs of the PS GL.

As the CDR regime is not yet operating, it is not possible to provide an exhaustive commentary on the adequacy of the PS GL. The views and recommendations in this ABA submission are based on the expected operating environment, which may prove to be different to the actual operating environment as new-to-market use cases are launched. In this regard, the ABA makes the following overarching recommendations in addition to the specific recommendations contained within the main submission:

- As the CDR is a 'ground up' development and it is not yet operationalised it is likely that there will be gaps in the PS GL. The ABA recommends that the PS GL undergo a second consultation twelve months after the launch of the CDR regime.
- Given the extensive referencing throughout the PS GL to other CDR documents which are subject to ongoing revision, the ABA recommends that the OAIC institutes a process for annual review (or as CDR documentation is revised) of the

PS GL in order to ensure that all cross-references remain up-to-date, complete, relevant and therefore effective.

- In addition to the requests for examples requested in the submission, as a general principle, it would benefit readers of the PS GL if the OAIC provided multiple examples where a Privacy Safeguard requires DHs and ADRs to consider what is 'reasonably needed' or 'proportionate'.

The ABA thanks the OAIC for the opportunity to consult with staff from the office during this process. Please contact me if you would like further clarification on the content of this submission.

Kind regards,

Emma Penzo
Policy Director

Encl.

Australian Banking Association

ABA Submission on the OAIC Draft Consumer Data Right Privacy Safeguard Guidelines

1. Key issues

1.1 Implications of dual privacy regimes

The ABA notes that the privacy impact assessment (**PIA**) process undertaken by Maddocks, has raised the potential that it is possible for a reading of the CDR legislation to conclude that data held by a DH becomes CDR data within the CDR Act once a sector is designated pursuant to instrument under subsection 56AC(2) of the CDR Act. While there will be Privacy Safeguards that apply to DHs generally, others will only be triggered by a valid consumer or product data request.

Given the complexity of navigating two privacy regimes, the PS GL should clearly outline the examples when data will be treated under the APP or the PS. For example, clarifying when a request to correct personal information should be treated under the APP or PS.

The ABA understands that the APP and PS apply to Data Holders as follows:

- If PS 11 applies to a Data Holder in respect of CDR Data, APP 10 does not apply to a Data Holder in relation to that disclosure of CDR Data (see section 56EC(4)(b) of the CDR Act);
- If PS 13 applies to a Data Holder in respect of CDR Data, APP 13 does not apply to a Data Holder in relation to that disclosure of CDR Data (see section 56EC(4)(c) of the CDR Act); and
- Other than the above changes to the application to the Privacy Act, APP 11 and APP 13 will apply to Data Holders in relation to CDR data (see section 56EC(5) of the CDR Act) and PS 1 applies in parallel with APP 1 such that a Data Holder would be required to have both a Privacy Policy and a CDR Policy (and we note that it makes sense that a Data Holder would be required to have a policy that outlines the way in which it manages CDR Data prior to a customer requesting such CDR Data).

The ABA is strongly of the view that the potential for misinterpretation needs to be addressed and clarified either through guidance from the OAIC which is consistent with figure 1: *Applications of Privacy Safeguards* or ideally through the amendment of legislation.

CDR Participant	Which Privacy Safeguards (PS) apply?
Data holder (DH)	PS 1 – applies concurrently to APP 1. PS 10 – applies to the disclosure of CDR data. There is no similar requirement under the Privacy Act 1988. PS 11, PS 13 – applies to the disclosure of CDR data and substitute for APPs 10 and 13 for disclosed CDR data.
Accredited person (AP)	PS 1, PS 3, PS 4, PS 5 – APPs apply concurrently(*), but with the more specific PS prevailing.
Accredited data recipient (ADR)	PS 1, PS 2, PS 6, PS 7, PS 8, PS 9, PS 10, PS 11, PS 12 and PS 13 – apply and substitute the APPs which do not apply to an ADR for CDR data that has been received under the consumer data rules or is derived from that data.
Designated gateway	PS 1 – applies concurrently to APP 1. PS 6, PS 7 and PS 12 – apply to the use and disclosure of CDR data under the consumer data rules and substitute for APPs 6, 7 and 11.

Figure 1: Applications of Privacy Safeguards[1].

(*) Per section 6E(1D) of the Privacy Act, for a small business operator who is an AP, the APPs only apply in relation to personal information that is not CDR data. The result being that for a small business operator AP who is also a DH of CDR data, the APPs will not apply in relation to that CDR data and the only PS that will apply are 1, 10, 11 and 13.

1.2 CDR complaints

The PS GL does not detail how the OAIC and Australian Competition and Consumer Commission (**ACCC**) will approach CDR regime complaints and how the complaints function of the OAIC will interface with the complaints heard by the Australian Financial Complaints Authority (**AFCA**). The ABA recommends that the OAIC's *Guide to privacy regulatory action* is updated to incorporate the intended approach, including the difference between how and what complaints will be handled by the OAIC, the ACCC and AFCA.

1.3 Grounds for refusal of a request for data

The ABA notes that the PS GL do not address situations where a data holder (**DH**) has a reasonable and legitimate concern about an accredited data recipient's (**ADR**) information handling practices and procedures. The ABA seeks guidance, with examples, in respect to acceptable grounds for a DH to refuse to disclose CDR data where there are reasonable and legitimate concerns.

[1] Source: Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum (link) p52

Australian Banking Association

2. Targeted feedback

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
Chapter A: Introductory matters	
A.24 and section: 'Which privacy safeguards apply to each entity'	It may be useful to note that organisations may be either DH or AP/ADR depending on the circumstance. The table referenced is at too high a level and does not demonstrate the nuance of the context to which the PS are to apply. For example, it does not capture the fact that one entity may be operating as a DH and an ADR at the same time for different sets of CDR data and therefore will have multiple obligations that apply concurrently. The table also notes that all PS apply to an ADR. However, PS 3 (which deals with soliciting CDR data) presumably does not apply to an ADR as an AP only becomes an ADR when it receives CDR data under the regime (see comments at B.4 of the PS GL).
A.26	'*In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.*' It would be helpful to understand at a principles level the OAIC's approach to managing the complexity in the interaction between the PS GL and the APP Guidelines. How does the PS GL intersect/interact with the APP Guidelines? Additionally, to what extent does commentary and guidance form the APP Guidelines become applicable to the OAIC's interpretation of the PS?

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
Definitions	**(a) Additional definitions:** The ABA suggests that additional definitions are required, particularly for the following terms: • CDR entity • De-identification • Data Recipient Accreditor **(b) CDR Data and Derived CDR Data:** The ABA recommends that the PS GL would benefit from the inclusion of examples of types of data that the OAIC would deem constitutes CDR Data and Derived CDR Data, including examples of directly and indirectly derived CDR data which reflect the difference between the two types, with particular reference to analytics and insights. **(c) Personal information:** The ABA recommends that the PS GL could be improved with additional commentary regarding the overlay of personal information and CDR Data. For example, in what circumstances could CDR Data also be personal information and how should participants deal with this overlap? Does it add or remove any obligations relating to the PS under which that data would normally be treated? The ABA recommends the inclusion of a section like C3 – How is CDR Data different to Personal Information? When may there be overlap?
Chapter B: Key Concepts	
B.4	The ABA seeks detailed clarification and examples as to whether CDR data (for example information about the user of a product including name and contact information) collected by an AP directly from the consumer in anticipation of making a CDR request to a DH will be treated as CDR data which they hold as a DH (assuming that they are an ADR of other CDR data).
B.12 – B.13	To the extent that Derived CDR Data generates Personal Information the ABA would welcome clarification on whether this would also be a 'collection'?

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
B.19 – B.20	The ABA welcomes further detail regarding the application of the term 'collection' within the CDR regime; For example: would it only be deemed a 'collection' when done so via the CDR processes.
B.25 – B.30	The PS affords protections to 'CDR consumers', which includes both individuals and businesses. Further clarity would be useful to make clear that a CDR consumer extends to business and additional commentary which would cover how these provisions would relate to an analysis for a business customer which is not currently undertaken under the Privacy Act (because the Privacy Act applies only to natural persons). The ABA refers to C18 as an example of the type of guidance regarding the application of the CDR regime to business which would be welcomed. Further detail on what constitutes a 'business account' in an individual's name is welcomed.
B.35 – B.41	B.35: The ABA recommends including examples of what 'relates to' and what does not 'relate to' a CDR Consumer according to the OAIC given the potential broad scope of this terminology. Also note the following in B41: 'By using the broad phrase 'relates to', the CDR regime captures meta-data.' The types of meta-data captured by the CDR rules and standards should be clearly outlined to ensure consumers are aware of what meta-data can permissibly be shared under the regime. Further, guidance should be provided regarding the interaction between the disclosure of meta-data and the data minimisation principles.
B.42 – B.46	B.42: The ABA notes that it would be useful to have examples of when a person is a CDR consumer by virtue of a supply of goods and services to that person's 'associates' bearing in mind the broad definition of associates and that a DH won't necessarily be able to identify the full range of associates without instructions.
B.47 – B.50	The ABA welcomes the connection to the APP Guidelines in B.48 and query whether this approach can be used in other definitions/terms?
B.55 – B.57	Does the consumer dashboard need to conform to any data standards? If so, the PS GL should note this requirement.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
B.77 – B.80	It is unclear why Consent and Authorisation is covered in this section and not in Chapter C. The ABA questions whether the commentary here should refer to Chapter C as that is the logical place in the PS GL for the detail relating to consent/authorisation.
B.101 - B.104	The ABA recommends that an example in this section would be helpful.
B.107	The ABA requests further guidance around circumstances where providing CDR data to a third party would be considered a use, rather than a disclosure. We note that the APP Guidelines touch on this issue in Paragraph 8.14.
B.139 – B.140	Given the expansion of the definition of 'use' it is important that the PS GL specifically notes the fact that this differs from the APP concept of 'use'. The PS GL requires further detail here. For example, to what extent will the APP guidance as set out in B142 – B144 be relevant?
B.141 – B.143	The ABA recommends setting out examples here, rather than referring to the Designation Instrument.
Chapter B General comment	Could a schematic of Chapter B be developed like that of Chapter C, Page 5?
Chapter C: Consent – The basis for collecting and using CDR data	
C.3 – C.7	The ABA recommends: • C.4 could be re-framed to be more like C.8 to make the distinction clearer. • Adding the time restriction as a difference (consents under the Privacy Act do not have a 12-month time limit under law).
C.35	This section is welcomed guidance.
C.39	Disclosing information about de-identification techniques may aid re-identification in some circumstances, including by malicious third parties. The ABA recommends additional guidance as to what level of detail is required in this notice to ensure consumers are informed about de-identification processes generally, without exposing them to unnecessary risk of re-identification.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
C.42 – C.43	The ABA seeks guidance as to whether the restriction on seeking consent set out in Rule 4.12 (3)(b) which prohibits the aggregation of data for the purpose of identifying, compiling insights in relation to or building a profile in relation to any identifiable person who is not the CDR consumer who made the CDR request (subject to Rule 4.12(4)) includes the application of insights gained from aggregated (and de-identified) data back to an identifiable person who is not the CDR consumer. For example, where aggregated and de-identified data is analysed to generate insights about a particular cohort of consumers and then these insights are linked back to an identifiable person because they fit within the particular cohort.
Chapter 1: PS 1 Open and transparent management of CDR data	
1.30	The ABA requests examples of how the 'reasonable steps' qualifications overlays with the different mechanisms that a DH and ADR need to put in place. Is there an implication that there is a difference in what constitutes reasonable steps for a DH as opposed to an ADR? If so, how does the OAIC propose to maintain the same standard across the CDR?
1.38 – 1.44	The ABA notes that under CDR Rule 7.2 [link] as currently drafted there is a requirement to have a separate CDR policy (to that of the Privacy Policy). The ABA notes that having two policies is not particularly consumer friendly and two policies may be confusing for consumers. The ABA recommends a single privacy policy, which incorporates either a section or an appendix on CDR, be adopted and would welcome OAIC feedback on this point.
1.43	DH will broadly treat individual CDR data as personal information in accordance with its Privacy Policy as it is generally bound by the APPs. Can a DH reference its Privacy Policy within its CDR Policy or is this likely to be considered user unfriendly? Specific examples or guidance would be useful as to what would comply with this high level guidance. The ABA recommends that the OAIC provides examples of the best way to avoid consumer confusion about handling CDR data as a DH.
1.47	The ABA is interested in specific examples/recommendations as to how this complexity can be appropriately communicated in a mobile friendly format.

Australian Banking Association

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
1.48	(a) The PS GL should provide guidance that such a statement of 'whether overseas disclosure is likely' complies with s 56ED(5)(f), or whether further information is required under PS1. (b) The ABA requests further guidance on what is meant by the requirement to include information in the CDR policy on 'events about which the CDR entity will notify the consumers of such CDR data' (s 56ED(5)(h)). (c) PS1 requires that ADRs must include information in their CDR policies as to classes of CDR data held including "information on product" and references s8 of the designation. S56EB of the Act states that the Privacy Safeguards only apply to CDR data for which there are one or more CDR consumers and so doesn't apply to information on the product referenced in section 8 of the designation instrument.
1.49	Disclosure overseas (third bullet point): The commentary in the bullet point is unclear as to whether the statement 'if it is practicable to specify those countries in the policy' relates to whether (a) it is impracticable to identify the countries at all because there are so many or (b) whether it is impracticable to specify them in the policy because there are so many and therefore they should be listed elsewhere or both. The first sentence in footnote 14 states: 'An example of when it may be impracticable to specify the countries in which service providers are likely to be located is where CDR data is likely to be disclosed to numerous overseas providers and the burden of determining where those service providers are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances.' The guidance then notes: 'If CDR data is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the CDR policy rather than in the body of the policy.' The ABA requests further clarity.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
1.49	De-identification of CDR data (fifth bullet point): The information to be provided is quite detailed and likely to only be useful to a sophisticated CDR consumer who has detailed knowledge of privacy issues. It would be more useful to explain to CDR consumers that de-identification: (a) is not an exact science but a risk based mechanism and (b) it is not impossible that an individual may be re-identified. It would also be useful to understand what level of information is required in relation to 'why the ADR asks for consents to de-identify CDR data' and 'the purposes for which ADR discloses de-identified CDR data.' Examples would be useful.
PS1 – General comment	There is a significant volume of highly complex information to be provided potentially in a mobile friendly format. The ABA recommends that the OAIC provides detailed advice for disclosures to consumers which will avoid information overload whilst communicating sufficiently specific information.
Chapter 2: PS 2 – Anonymity and pseudonymity	
2.9 – 2.13	The ABA welcomes more examples as per Chapter 2, Page 6, which capture the complexity of this regime.
Chapter 3: PS 3 Seeking to collect CDR data from CDR participants	

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
3.8 – 3.9	An AP is only an ADR where it has received CDR data under the CDR regime (see s 56AK of the Act). As an AP, APP 3 will apply to any personal information handled by them including where that CDR data has not been obtained under the CDR regime by that AP (per example given at Chapter 4.16, Page 6) unless they are a small business for the purposes of the Privacy Act. It would be helpful to describe the changing nature of an AP's role as dictated by its relationship to particular CDR data. If a person thinks of themselves only as an ADR after they have first received CDR data under the regime, they run the risk of not complying with broader provisions. Given the complexities associated with parallel regimes and the statements made in the PS GL on the interaction between the APPs and PS, the ABA recommends the presentation of real world examples which could be used to provide guidance for participants on the application and nuance of the regime. For example, the following statement (and corresponding footnote) in Chapter 3, Page 4 would benefit from a concrete example: 'APP 3 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data. All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.'
Chapter 4: PS 4 Dealing with unsolicited CDR data from CDR participants	
4.17 and 12.100-12.102	Does the option to put CDR data beyond use (as it applies to PS 4 and PS 12) apply even if the data is not held in a backup system?
4.8	'It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs)'. Note that this text includes an incorrect reference to PS 12 – should be PS 4.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
4.16	Comment on the provided example: The last sentence states that 'if Brent is an APP entity' he must also comply with the APPs. However, as Brent is an AP he will have to comply with the Privacy Act per s 6E(1D) of the Privacy Act i.e. in relation to any personal information that he holds which is not CDR data. This has the perhaps unintended consequence that if Brent is a small business, he will not need to comply with the Privacy Act in relation to the CDR data that he receives outside of the CDR regime and nor is he subject to many of the privacy safeguards which relate to the use and disclosure of the CDR data and the protection of the CDR data but he will be subject to the Privacy Act for personal information which is not CDR data. Further guidance on this point would be useful.
Chapter 5: PS 5 Notifying of the collection of CDR data	
Chapter 5 – General comment	Given that CDR receipts also need to be provided at the point of collection, the ABA recommends providing further guidance in this chapter, including in respect to how these receipts interact with the consumer dashboard. More generally, a section of the PS GL should comprehensively address the various notice requirements under the regime given their complexity.
Data Minimisation principle	The ABA notes that the industry requires greater clarity on the data minimisation principle and how it is to apply in practice. Do the same relevant considerations in determining whether a collection is 'reasonably necessary' under APP 3 (as outlined in paragraphs 3.17 – 3.21 of the APP Guidelines) apply to CDR data?
Chapter 6: PS 6 Use or disclosure of CDR data by accredited data recipients or designated gateways	
6.15	The ABA requests further guidance on this scenario; in particular, when the act would be considered a disclosure over a use.
6.34	How is 'reasonably needed' determined in practice? It is recommended that the PS GL provide further examples on what disclosures would not be proportionate to the purpose for disclosure.
Chapter 7: PS 7 Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways	

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
Direct Marketing	The PS GL includes the following example of what does not constitute DM: *'A consumer is considering switching providers for a product. The consumer provides an accredited data recipient with a valid request to seek to collect their CDR data from their current provider (the data holder) and use that data to provide suitable offers in relation to the product. In doing so, the accredited data recipient uses the CDR data to provide the good or service. This use is not direct marketing and Privacy Safeguard 7 does not apply. The accredited data recipient must comply with Privacy Safeguard 6.* What is the OAIC's position where offers are provided in relation to a related product or service that the ADR considers would be suitable? The ABA would welcome guidance on this topic. Given that part of the CDR's success is premised on the offer of goods and services to customers, arising out of the CDR regime, guidance on what is permissible in this context will be important to guide the operation of the CDR.
Chapter 8: PS 8 Overseas disclosure of CDR data by accredited data recipients	
Chapter 8 – General comment	The ABA recommends that the PS GL address whether there could be scenarios where the act of sending information overseas could be considered a use, rather than a disclosure.
Chapter 8 – General comment	Paragraph 8.14 of the APP Guideline provides some examples of provisions that should be included in contractual arrangements for overseas disclosures, do these also apply when considering the 'reasonable steps' exception under PS 8?
8.2	Replace 'condition 2' with 'paragraph 8.1(b)' for clarity.
8.16	The ABA recommends that the PS GL confirm whether the definition of a related body corporate is taken from the Corporations Act 2011.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
8.28 – 8.31	Disclosing CDR data with a 'reasonable belief' the overseas recipient is subject to a substantially similar law (and the consumer can enforce that law). The ABA notes that this exception is broadly comparable to the exception in APP 8.2(a). While the ABA appreciates the intent of this exception – to facilitate the free flow of information across borders – in practice, entities are rarely able to rely upon it. Without conclusive guidance from the OAIC, which specifies which schemes meet the required threshold, it is too risky for entities to make their own assessment. The ABA recommends that the OAIC introduces a list of schemes that would meet the requirements under APP 8.2(a) and PS 8 to provide entities with certainty so that these exceptions can be used as intended. Similar approaches are undertaken in Europe, where the European Commission lists countries that offer an adequate level of data protection.
Overseas disclosures and Outsourcing arrangements	The ABA asks: • what steps need to be taken to ensure that CDR data is appropriately handled in CDR outsourcing arrangement? • what constitutes a 'substantially similar law or binding scheme' for the purposes of PS 8?
Chapter 9: PS 9 Adoption or disclosure of government related identifiers by accredited data recipients	
9.1 and 9.26	The ABA recommends specifying the Act under which the relevant regulations apply.
9.15	The ABA requests further guidance on how the CDR regime interacts with the *Privacy (Tax File Number) Rule 2015* and whether TFN information can be included in CDR data. By way of example, government identifiers may be inadvertently collected or disclosed in a way that cannot be identified or is not directed by the DH or ADR. For example, where a consumer inputs a TFN in a free-text transaction description field which is subsequently shared as part of their transaction history. Additionally, the CDR extends to business consumers and guidance should be provided on how the CDR regime interacts with various laws that apply to the collection, use or disclosure of government related identifiers for business consumers.
9.28	Heading '*Privacy Safeguard 4'* should also refer to Privacy Safeguard 3.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
Chapter 9 – General comment	The 'Data Dump Pty Ltd' example in Chapter 9 could provide more clarity around whether APP 4 alone or whether PS 4 obligations also apply.
Chapter 9 – General comment	It would be helpful to include an example where government related identifiers could be transferred in accordance with PS 9.
Chapter 10: PS 10 Notifying of the disclosure of CDR data	
10.8	If a DH or ADR is complying with the CDR Act including the Rules in relation to disclosing CDR data (personal information) it is assumed that they will be complying with APP 6 with regard to disclosing this data. If this paragraph is trying to highlight something else i.e. where they have other personal information which is not CDR data it would be useful to highlight that with an example.
10.10 – 10.11	A considered approach to notification of joint account holders is required: Is it adequate to notify by updating the consumer dashboard in the case of joint account holders? A joint account holder may be unaware of the authorisation by the other account holder so may not check or even be aware that they have a consumer dashboard. It may be appropriate to notify joint account holders electronically when data sharing is authorised. However, a DH will not be required to notify the non-requesting joint account holder/s where the DH considers this necessary to prevent physical or financial harm or abuse. The ABA recommends further guidance is provided that following the DH's existing procedures or process for individuals experiencing family violence is sufficient to meet the exception to notifying other consumers of the CDR data, where these circumstances apply.
10.19	It would be useful to have an example or additional guidance as to what needs to be noted in the consumer dashboard to drive a minimum level of consistency and to reinforce that a description of 'what CDR data was disclosed' does not require a true copy of the data but a description of the type of data, across a particular time period e.g. transaction data relating to a particular account since the Earliest Holding Date.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
10.22, 10.23, 10.24	The ABA notes that this information is too granular and may be confusing to a consumer. The ABA recommends that compliance with the CX Guidelines is sufficient (ie the dashboard will contain the date of consent and that the disclosure was for a single occasion or ongoing). There is an additional control in that if a customer is concerned about the precise date of disclosure, the customer can request access to the DH's records under Rule 9.5.
10.25	The frequency of collection is known by the ADR and may vary during the period of consent. The ADR is required to provide this information on its dashboard. The DH will not know how frequently data will be pulled within a specified period as a DH obtains an authorisation for data to be disclosed over a particular period with the ADR being able to pull data monthly/weekly/daily at their discretion (see CX Guidelines). This guideline appears to require a log of access, which is confusing and unnecessary. The ABA recommends that compliance with the CX Guidelines is sufficient ie the dashboard will contain the period of consent and that the disclosure is ongoing for the period of consent. There is an additional control in that if a customer is concerned about the precise date of disclosure, the customer can request access to the DH's records under Rule 9.5.
10.26	The ABA recommends that paragraphs 10.20-10.26 of the PS GL are deleted and the new 10.20 reads as follows: 'This requirement will be met if the data holder complies with the relevant sections of the Consumer Experience Guidelines'.
Chapter 11: PS 11 Quality of CDR data	
11.2	PS 11 provides that holding CDR data so that it can be disclosed as required under the CDR is not a purpose when determining the purposes for which the CDR data is or was held. The ABA requests an example to illustrate how this provision applies.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
11.5	Why is it important: It would be useful to clarify that entities may be required to correct inaccuracies in their data after it is shared where the data was inaccurate at the time of the disclosure (as distinct from where it is no longer accurate after the point of disclosure). e.g. An unauthorised transaction may appear in the records shared and is correctly recorded as a transaction at the time, notwithstanding the fact it is later reversed. It would be useful to clarify that this is not inaccurate at the time of the sharing.
11.11	The ABA notes that: • that an APP entity's obligations under APP 10 about use and disclosure is that data is accurate, up to date, complete and relevant having regard to the purpose of the use or disclosure. • APP 10 does not include holding the information for the purpose of the CDR regime (i.e.: APP 10 does not apply to a disclosure under the CDR regime).
Page 5	**Summary of application of PS 11:** Guidance would be useful as to the application of PS 11/APP 10 where a DH declines to disclose CDR data despite being authorised to disclose under the Consumer Data Rules. It is assumed that PS 11 still applies as 56EN(1) is framed as being required or authorised to disclose under the rules.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
11.15	'PS 11 requires a data holder to take reasonable steps to ensure the CDR data is, having regard to the purpose for which it is held, accurate, up to date and complete'. Accuracy will be assessed in the light of the purpose for which the information is held and not the purpose for which it is shared. It would be useful to have examples to clarify this. E.g. small errors in CDR data may be immaterial for the purpose for which the DH holds the information and will not necessarily make it inaccurate for the DH. The mere fact that these small errors may have greater implications in the context of and ADRs use of the data is not relevant. Whilst APP 10 has a "purpose" test, that test applies to disclosure in a way that it does not under the CDR regime. Consumers could be confused as to how the quality requirement operates under the CDR regime. Further guidance should be provided which will confirm that a customer's details are considered to be accurate if recorded in accordance with the customer's instructions (and KYC requirements) at the time of the customer's disclosure. If a customer changes their mobile number, for example, but does not inform the DH, the old mobile number should not be categorised as 'inaccurate'. Where the customer updates their details, this should be referred to as an update, it is not a correction.
11.16	Accuracy of CDR data: There is reference to stating the bases of the estimation as a defence to an allegation that CDR data is inaccurate. Guidance/examples would be useful as to the level of information required regarding the logic behind an algorithm.
11.17	CDR Data is required to be up to date. There may be data latency issues for some CDR data. This will mean that there may be up to a 24 hour lag for certain CDR information. For example, the updating of personal information and the opening of an account may take up to 24 hours to be available to be able to be disclosed. The PS GL should allow for a short time lag and for data to still be considered 'up to date'.
11.18	As with accuracy of 'CDR data' in 11.17 above it would be useful to have examples which address the 'purpose for which it is held test'.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
11.20	The PS GL provides an example in relation to a debt being repaid. DH's are limited to the duration or time period for which the ADR requests data. As such, the data may present a misleading picture. For example, where the consumer has repaid the debt or taken out another loan, but the period of collection did not capture this information.
11.26	It would be useful to have more emphasis on the 'purpose for which data is held test' in this section. The disclosure of this data under the CDR regime is not a purpose for which the data is held. Whilst it is likely that the purpose for which a DH holds sensitive information requires that information to be accurate, it is not ensuring the accuracy of the sensitive data because it is disclosing it under the CDR regime. The point of disclosure of the CDR data is the time at which a DH must ensure it has taken reasonable steps rather than the reason it must ensure quality.
11.28	'The following are given as examples of reasonable steps that an entity should consider - Ensuring internal practices, procedures and systems are commensurate with reasonable steps to ensure the quality of CDR data the entity is authorised or required to disclose.' The example provided by the OAIC uses the term 'reasonable steps' to define 'reasonable steps'. The circularity should be removed and more specificity used in explaining the concept of 'reasonable steps'.
11.43	Consider clarifying whether if an ADR receives CDR data outside of the CDR regime (and therefore is not an ADR for that particular CDR data but may be for other CDR data) (see example Chapter 4 ,Page 6) APP 10 will apply to the ADR for that other CDR data.
11.45	The wording should be amended to: 'Privacy Safeguard 11 requires a data holder to make available for disclosure corrected CDR data to the original recipient of the disclosure if…' This is because the only way a DH can disclose corrected data is by making it available in an API. The ADR must then call the API for the corrected data. There is no mechanism in the standards that provides for a DH to 'push' this information to the ADR without it first being requested.
11.50	The record of the separate disclosures will be kept but the disclosures cannot be tagged as 'correct' or 'incorrect'.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
Chapter 12: PS 12 Security of CDR data, and destruction or de-identification of redundant CDR data	
12.15	'The terms 'misuse', 'interference', 'loss' and 'unauthorised access' are not defined in the CDR regime. The following discussion represents the OAIC's interpretation of these terms based on their ordinary meaning. However, given that information security is an evolving concept, the discussion below is not intended to include an exhaustive list of examples.' The ABA agrees that information security is ever evolving and suggests updating the APP Guidelines with some of the more recent examples that are included in this list.
12.15	Unauthorised modification occurs where CDR data is altered by someone who is not permitted to do so, or where the data is altered in a way that is not permitted. For example, **unauthorised access** would occur if an employee of an ADR or designated gateway altered a consumer's savings account information to offer a more favourable deal. The reference to 'unauthorised access' (in bold for accent) should be 'unauthorised modification'.
12.34 Footnote 16	The definition of 'enforceable' is a key definition. The ABA suggests that it is moved to the body of the PS GL. The ABA also queries whether 'construal' is supposed to be 'contractual'.
12.87 – 12.95; **12.100 – 12.102;** **12.106 – 12.109**	Step 5 provides useful guidance. The ABA recommends that it would be helpful for the OAIC to provide guidance on the meaning of 'put beyond use' within this section. The ABA notes the interchangeable use of 'deletion' and 'destruction', which are distinct concepts. The ABA has previously noted that 'deletion' is arguably a lesser standard than 'destruction'. Further guidance and clarity on these issues is welcomed.
12.100-12.102	The ABA supports the scenario where CDR data can be considered 'destroyed' if it is put 'beyond use'. This guidance is consistent with the OAIC's *Guide to securing personal information.*
12.106	As advances in technology mean that de-identified information today may not be considered de-identified in years to come, the ABA recommends that the PS GL confirms that this determination of the ADR is a point in time assessment.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
12 - Part B	The ABA highlights that customer consent is not given on an account level. This means that a customer may have consented to the collection of transaction data for several accounts. Please provide examples of how the deletion/deidentification requirements apply to the different states of consent (e.g. withdrawn, expired).
Chapter 13: PS 13 Correction of CDR data	
Chapter 13 – General comment	The statement 'Where a data holder has not received a correction request' should specify 'a correction request made under PS 13'.
13.12	We note that fraudulent transactions will not be captured as a 'correction' because technically the data is not incorrect as the withdrawal of funds did take place. After the fraud is detected, there will be a refund to the customer's account of the amount. The refund, which will be made on a later date, will be reflected in the data.
13.21	The DH may consider that the data is accurate, up to date and complete and not misleading for the purpose for which the DH holds it. The test should be whether it is necessary for the DH's purposes to record the updated/corrected data.
13.23	*'…the entity is an accredited data recipient of the data and the request is in respect of data the entity has collected from a data holder (rather than data the entity may have derived from collected data)'.* For clarity, this point should specify that the reason is because the DH should be receiving the request.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
13.23	Reasons for not correcting CDR data: Reasons should include statement 'where the data is considered correct for the purpose for which the data is held' with associated examples. For example: • fraudulent transactions which are correctly recorded as a transaction in relation to an account and which, where found to be fraudulent, will be reversed in a subsequent transaction. • where a customer's financial position may be incomplete in that it does not disclose other liabilities, which don't appear as transactions in the accounts.
13.30	The example relating to fraudulent transactions in not appropriate. See comments above in 13.12.
13.34	Factual information which is inaccurate for the purpose for which it is held. It is possible that employment status information may be inaccurate but was accurate at time of credit decision and may no longer be relevant to banking service provided by DH. Accordingly it is not inaccurate for the purpose for which it is held.

Report Section (Paragraph/Page Reference)	Feedback & Recommendation
13.40	As an example of where CDR data may be misleading, but is accurate for the purpose for which it is held: A customer with a home loan may have a redraw feature and be making repayments above the contractual minimum. However, the apparent amount available for redraw (which would appear on electronic banking interfaces will fluctuate over the repayment cycle notwithstanding the regular payments. This might be due to interest being charged or adjusted, payments from other sources being cleared or whether the repayment for that cycle is still pending. The records would be accurate for the purpose for which it is held, that is informing the customer of the amount available at that point in time, but by the end of the statement period the situation at that past date may have been adjusted, so that it appears at variance with a now “inaccurate” past record. Another example would be that the customer holds two dormant credit cards, and in discussion with a branch manager requested these be closed in contemplation of a home loan application. At the same time, the customer requested the CDR data on all accounts to be shared with a broker. The dormant credit cards had not been removed and this impacted negatively on the customers’ ability to secure a home loan. In this case the information was inaccurate for the purpose for which it was held.