Consumer Data Right

Data Standards Advisory Committee (DSAC)

Minutes of the Meeting

Date: *Wednesday 27 September 2023*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Committee Meeting # 56*

Attendees

Committee Members

Andrew Stevens, Data Standards Chair
Alysia Abeyratne, NAB
Jill Berry, Adatree
Damir Cuca, Basiq
Chris Ellis, Finder
Prabash Galagedara, Telstra
Melinda Green, Energy Australia
Peter Leonard, Data Synergies Pty Ltd
Greg Magill, Westpac
Colin Mapp, Toyota Finance Australia
Lisa Schutz, Verifier
Aakash Sembey, Origin Energy
Zipporah Szalay, ANZ
Tony Thrassis, Frollo

Observers

Louise Staker, DSB
James Bligh, DSB
Ruth Boughen, DSB
RT Hanson, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Tim Jasson, ACCC
Seamus O'Byrne-Inglis, ACCC
Sarah Croxall, OAIC
Shona Watson, OAIC
James Kelly, Treasury
Aidan Storer, TSY
Lyria Bennett Moses, UNSW Sydney

Apologies

Stuart Stoyan, Fintech Adviser

Chair Introduction

The Data Standards Chair (**Chair**) opened the meeting and thanked all committee members and observers for attending meeting # 56.

The Chair acknowledged the traditional owners of the various lands from which the committee members joined the meeting. He acknowledged their stewardship and ongoing leadership in the management of water, land and air and paid respect to their elders, past, present and those emerging. He joined the meeting from Cammeraygal land.

The Chair noted that Maintenance Iteration # 17 has commenced and the Decision Proposal for Maintenance Iteration # 16 has been circulated to the Data Standards Advisory Committee (**DSAC**) for feedback.

The Chair welcomed Prof Lyria Bennett Moses from the UNSW Sydney (**UNSW**) Law and Justice faculty. The Data Standards Body (**DSB**) commissioned UNSW to conduct some research around Information Security Risk in the context of the Chair's responsibilities as the Data Standards Chair. Lyria was in attendance to present the findings from that research.

The Chair noted that the next DSAC refresh is coming up on 30 November 2023 and the DSB will be reviewing the composition of the committee over the coming month. He asked members to let the DSB know if they are interested in continuing their membership.

The Chair noted that Greg McGill from Westpac has resigned from the Committee from 3 October 2023 as he is moving into a new role. Consumer representatives Chandni Gupta (CPRC), Deen Sanders OAM (Deloitte) & Drew MacCrae (Financial Rights Legal Centre) have also withdrawn from the DSAC on the basis that they don't have the resources or the capability to evaluate and contribute at the level they'd like. The Chair is considering the important issue of consumer representation, with the help of Treasury (**TSY**).

The Chair thanked outgoing members for their valued contributions to the committee and wished them well.

The Chair noted that two new roles with the DSB Team have been advertised – Assistant Director, Cyber Assurance and Assistant Director, Compliance.

Lastly, Barry Thomas the General Manger of the DSB has stepped down from his role at the DSB. Barry has made an outstanding contribution to the CDR, the DSB and to the Chair and he will be greatly missed.

Louise Staker will be leading the DSB team until the new General Manager, Naomi Gilbert, commences at the end of October.

Minutes

Minutes

The Chair thanked the DSAC Members for their comments on the Minutes from the 12 July 2023 meeting. The Minutes were formally accepted.

Action Items

The Chair noted that all Action Items were either covered-off in this meeting or had been completed.

Data Standards Chair's Response to the UNSW Reports

Background

The Chair noted that, consistent with his commitment to total openness in terms of consultations, standards development, decision making and ongoing operation and maintenance type activities, it is both appropriate and necessary to engage independent input and perspectives.

The DSB has commissioned UNSW to conduct some research around the components that will ultimately form the Information Security Risk Framework, including how to operate the framework. UNSW delivered two reports, Report 1: Considerations for Managing Cyber Threats to the Consumer Data Standards: A Report to the Data Standards Chair and Report 2: Risk Management for the Consumer Data Standards: A Report to the Data Standards Chair.

The Chair noted that, given the standards are made in the context of the CDR rules, some risk management and threat implications may not be confined to the standards. That is an area UNSW spent a lot of time looking at. He noted that the reports are for the Data Standards Chair and they have been deliberately focused on his responsibilities. However there are implications, learnings and perspectives for the broader CDR agency and CDR programme.

The DSB thanked UNSW for this work and also thanked Peter Leonard for his contribution as a privacy representative. Based on the recommendations from the report, PwC's Indigenous Consulting have been engaged to do work on data sensitivity, which is close to finalisation. This will be made public in due course. The DSB is also undertaking work to respond to UNSW's recommendations in relation to privacy. In addition, the two new Assistant Director roles will form part of the Digital Trust team and are being recruited in response to the reports. The DSB is also working with the other CDR agencies to consider cross-agency risks and uplift cyber risk capability.

UNSW Presentation

Prof Lyria Bennett Moses from UNSW commended the openness in the data standards development process and the engagement with stakeholders, which supports public confidence in the CDR as a whole. She presented the high-level findings and recommendations from the two reports.

Threat Report

The Threat Report looked at i) threat assessment and drew on ii) expertise in computer science, security engineering, threat assessment, the cyber threat landscape, law and policy.

It examined the threat landscape in the context of the CDR, threat modelling (what it is, why it matters, how to do it and resourcing) and made the following recommendations:

1. Conduct threat modelling – independent, ultimately transparent
2. Do internal/independent modelling at least every 2 years, also in response to significant changes and incidents
3. Data Standards Cybersecurity Expert Advisory Panel

4. Collaboration and sharing among bodies involved in CDR governance
5. Use a wide lens, including whole data lifecycle, consumer interfaces with the system, social engineering, threats to capability
6. Establish capability for security and threat assessment functions
7. Data Standards Safety System – "have a plan" to manage attack or crisis, regular coordinated drills/evaluation
8. Methodology
   - OWASP-TMP Threat Modelling methodology
   - STRIDE Threat Classification framework

UNSW noted that they did not artificially limit the report to matters within the Data Standards Chair's remit but looked at systemic risks across the program where relevant, including the risk of undermining the perceived trustworthiness of CDR system.

The DSB noted the complexity of the environment, and the fact that CDR is a new system, and thanked UNSW for recognising this. The DSB is continuing to build its capability to respond to the identified risks.

One member is interested in how the participants of the CDR can contribute to this exercise.

UNSW noted the importance of working together in the context of shared risks. In the context of the Threat report, this goes to information sharing. The other important piece is the recommended Data Standards Safety System, which would need cross-agency involvement, including coordinated drills and evaluations.

The Chair noted that the report emphasised the importance of collaboration with participants and other organisations and he has accepted all those recommendations. He has a total commitment to openness and to collaborating with participants at all times. Now it's a question of how to put a process around that to make it effective.

One member asked about security risks other than risks associate with cyber-attacks. UNSW noted that the report deals with internal threats as well as external threats (that is, from organisations and individuals inside the system). This goes to the recommendation about applying a broad lens to the threat assessment.

One member noted that in the energy sector, they are concerned about increased risk of fraud associated with setting up accounts through digital channels. As we open up the CDR, this is something we need to tackle, otherwise there is a vulnerability which the CDR just exacerbates.

UNSW noted that this report was not a threat assessment but an overview of the threat landscape and highlighting why it is important to do the threat assessment. However, that example highlights the importance of looking at these issues holistically.

The DSB noted that the Chair has also been considering the report's recommendation to set up a Data Standards Cybersecurity Expert Advisory Panel. Without pre-empting the Chair's decision, they are looking at the composition and expertise that might be required.

<u>Risk Report</u>

The Risk Report looked at i) risk governance issues and ii) expertise in risk management/governance, privacy (law, impact assessments, rights) data governance, law and policy, and the role of standards.

The themes of the risk report are that:

- risk governance is critical, particularly given the threat landscape identified by the threat report
- risk governance in the CDR is hard and complex, partly because risks are shared and there are lots of different players, with a divergence in cyber risk maturity.

The Risk Report recommendations are:

1. Ensure risk governance for the CDS
   - Responsibility of Chair as an official responsible for day-to-day risk
   - Aligned with RMF for TSY, but possibly separate
   - Security risk management aligned with TSY security plan
   - Specific allocations of responsibility to those with expertise. Separate CSO?
2. Legal Compliance
   - Ensure Data Standards are 'binding' where required
   - Clarify applicability of DTA digital oversight framework
3. Use accepted methodologies for security risk management e.g. ISO IEC 27005
   - Address shared risks
   - Broad lens, including unauthorised handling by CDR participants and external threats
   - Develop common use cases, use to consider scope/quality of consents and operational processes
   - Recognising potential for harm from internal/external threats, recognise where risk is high/extreme
   - Collaboration and transparency regarding shared risks
4. Consider impact, even of 'technical' data standards, on consumer and human rights
5. Trigger Privacy Impact Assessments as required
   - Should be broad, holistic, scheme-wide view rather than layering of particular views
   - Should look to data standards and other levers

UNSW noted the role of trustworthiness in ensuring social licence to operate and, ultimately, success.

One member noted that the CDR is only as good as its weakest link. They asked if UNSW had any commentary about reporting and enforcement as part of the risk assessment.

UNSW noted that the risk report is not a risk assessment but does highlight the importance of a broad approach to understanding risks.

UNSW noted that many of the challenges of data in its life cycle arise through over exposure of information that has been received into an organisation and over-retention of information within an organisation. Latitude Financial is a good illustration of both of those risks. UNSW could have narrowed the focus of the report to only examine matters within the Chair's remit but they elected not to do so because it's important to look at data risk through the data life cycle. The broader issue is risk to the perceived trustworthiness of the CDR system. It is important that risk is appropriately managed, including in particular at those endpoints of overexposure of CDR data when received, and after it safely passed through the system, and over-retention of data.

One member noted that some of the risks identified would amount to a breach of the CDR Rules and other requirements. For example, the CDR Rules require consumers to explicitly provide consent in relation to how their data will be used, meaning that any secondary use is not permitted and would be a breach of those rules. The member also asked how to situate the report in the context of encouraging adoption into a system that is safer than other mechanisms.

UNSW agreed with the point and noted that there is a question about how the reports should be released to ensure clear communication and to avoid unnecessarily setting off alarm bells. The risks of CDR, for example, do not compare with the risks of credential sharing and screen scraping.

The Chair noted that he did not originally intend to make a public statement but is reconsidering this position in light of these points. DSB will work with DSAC members and UNSW to prepare a statement. It would be unfortunate if the outcome of the release of this report was a suggestion that CDR compares unfavourably with other regimes, which is not the case and was not the intention of the report.

The Chair thanked Lyria Bennett Moses for the presentation and the tremendous piece of work from the UNSW team.

Working Group Update

A summary of the Working Groups was provided and these DSAC Papers were taken as read.

Technical Working Group Update

An update was provided on the Technical Working Group by James Bligh:

The DSB thanked the organisations that participated in the recent Non-Functional Requirements (**NFR**) Workshops. There was a lot of consensus and very helpful feedback on the need to change the consultation processes to accommodate NFRs. In particular, the community suggested a working group with a consistent membership, which includes members of the community. The DSB is considering a trial, followed by a retrospective and then set up a more formal structure.

The Decision Proposal for Authentication Uplift has gone live. It is a complex high level decision proposal and will be followed by a series of much more targeted proposals based on community feedback.

Consumer Experience (**CX**) Working Group Update

An update was provided on the CX Working Group by Michael Palmyre:

The DSB presented on the hypothetical state of CDR consent in the last month. This included a roundtable run with TSY at Intersekt on screen scraping and the CDR consumer experience. The DSB and TSY also ran a stakeholder forum on the consent review and CDR future state, the slides of which were published in the Design Paper: CRD Consent Review.

The DSB noted that the Design Paper included wireframes around a hypothetical state including the ADR-side consent review change proposals; authentication uplift (demonstrating app2app flow in the banking sector); and DH side account specification improvements based on FAPI 2.0, Rich Authorisation Request functionality.

Stakeholder Engagement

A summary of stakeholder engagement including upcoming workshops, weekly meetings and the maintenance iteration cycle was provided in the DSAC Papers, which were taken as read.

Presentation on Consent Continuity

Tony Thrassis, the Chief Executive Officer of Frollo presented on Consent Conversion in the Consumer Data Right as follows.

Over the last 6 months, when a consent has not been successful Frollo has asked consumers why this was the case.

An average of 27% of collected consents do not succeed after the consumer has been redirected to the bank. This is based on 62,142 consent authorisation requests between March and August 2023 across 111 data holders.

Frollo conducted a consumer survey with the following response results:

- There was an issue logging in to the bank (231 respondents)
  - I got an error when I tried to login to the bank (90 respondents)
  - I never received my OTP or my OTP didn't work (93 respondents)
  - I did not know my bank login ID (10 respondents)
  - Other (38)
- There was a technical issue and the process has failed (421 respondents)
  - I got an error message and could not continue (193)
  - I was able to share my accounts but it was not sent back to Frollo (63 respondents)
  - I never got sent to the bank website to link my accounts (57 respondents)
  - Other (105)
- There was an issue selecting the bank accounts (83 respondents)
  - I did not see one or more of the accounts I wanted to link (55 respondents)
  - I decided not to link my account (2 respondents)
  - Other (26 respondents)

The results from the user survey with people whose consent failed on the Data Holder side showed:

- Can't login to bank (48.5%) – Main issue: OTP. Other issue: user never reached the bank website
- Issue after logging in (34.7%) – Main issue: Error after logging in, could not continue. Other issue: User was never sent back to the Frollo app
- Can't select accounts (11.9%) - A mix between joint accounts, business accounts and superannuation. Some responses only said account wasn't eligible for sharing
- Other (5%)

Frollo noted that a lot of the results point to technical difficulties, including difficulties with OTPs and in navigating data holder web pages for the purpose of giving an authorisation. They noted that there are no standards in regard to web pages and suggested review of how data holders are presenting the authentication pathway to consumers. Frollo will publish the slides on their website.

One member noted there's ultimately a lot of inconsistency and non-compliance in the information displayed to consumers on data holder web pages. They think it is important there are requirements

about what needs to be on these pages and associated record-keeping requirements, like there are requirements for CDR representatives and principals to keep screenshots and videos of their processes.

The DSB noted that this is very aligned with feedback DSB and ACCC have received from stakeholders. This feedback led to Get Metrics v5, which split out tiers and will hopefully start identifying these issues more systematically. The DSB noted one of the issues raised in that consultation was calls to the PAR end point that don't successfully then complete an authorised endpoint call. They asked whether the 49% that don't succeed at login includes that or is that a separate number?

The Chair asked Frollo if they would be willing to share more detailed information with the relevant data holders on a confidential basis, if requested.

Frollo would be happy to share on a confidential basis. They'll be starting to work with data holders bilaterally, and with the ACCC, to collect request URIs and pass these on to data holders to help them investigate why people are dropping out of the authorisation process.

The Chair noted that a one in four failure rate at this point is not consistent with a frictionless consumer experience. This is something that needs attention.

The DSB noted that there is a lot of dots to connect with the work that is happening so it's a good time and a great opportunity to funnel these into existing consultations, including the authentication uplift consultation. If 50% of the issue is the consumer not being able to log into their bank, the authentication uplift may be a solution, particularly given that App2App in the banking sector is an expected outcome.

The DSB noted that for the issues with logging in, it would be useful to hear more details around that, but for the most parts it sounds like they stem from implementation or compliance, as opposed to rules or standards requirements. Where the feedback is that consumers can't select an account, the operational enhancements rules consultation paper includes a question asking if the rules should automatically make account administrators nominated representatives for business accounts, which may go to this issue. There may also be a broader eligibility question which would be worth exploring in more detail.

One member expressed the view that this needs to be tackled as an operational issue. In terms of App2App, they cautioned that it won't assist in the majority of use cases for CDR because it assumes bank to bank data transfers. They wouldn't want to see the DSB divert too much from addressing the issues identified on the assumption that App2App is the way of the future and will resolve the concerns raised.

Issues Raised by Members

No issues were raised this month.

Treasury Update

Aidan Storer, Assistant Secretary, Market Conduct and Digital Division (**MCDD**) provided the TSY update:

TSY noted that a number of CDR Rules consultations are open including the Expansion to the Non-Bank Lending sector and the Consent Review and operational enhancement design papers. They have held stakeholder forums and information sessions at Intersekt which were well attended, and held multiple bilateral meetings with stakeholders on those consultations.

TSY noted that some of the feedback received on NBL had been around the proposed implementation dates for CDR obligations, the de minimis threshold and what particular data holders would be captured, and the proposal to carveout hardship data. They are looking forward to further feedback.

TSY noted that on the operational enhancements design paper, they've had some feedback around the practical implementation of the proposed change to the ACCC's monitoring and enforcement powers for CDR representatives, and the proposed obligations for CDR representatives and OSPs to handle all data they receive from their ADR principal as service data.

TSY noted on the consent review design paper, the feedback has been broadly positive towards proposals to streamline the consent process and improve consumer experience.

TSY noted in terms of next steps, they will analyse all the feedback and, in consultation with the other CDR agencies, prepare final rules to extend CDR to the NBL sector which they will put to the Minister at the end of this year or early next year for decision. Following consultation on the design papers, TSY will work on a package of draft rules for consultation late this year or in the first quarter next year.

TSY noted that a discussion paper on screen scaping is out for consultation, with submissions due by 25 October. This follows the Government's response to one of the recommendations in the Statutory Review of the CDR, which is to consult on policy options for regulating screen scraping, or even banning it where CDR is a viable alternative.

ACCC Update

Tim Jasson, the Executive Director of the Consumer Data Right Division at the Australian Competition and Consumer Commission (**ACCC**) provided an update:

ACCC noted that Daniel Ramos has temporarily moved to lead the work on the ACCC's digital identity for the remainder of the year. During this time Tim Jasson will be acting for his CDR duties.

ACCC noted that in regard to Frollo's presentation, ACCC are aware of those issues reported regarding the authorisation processes and they continue to consider those as compliance matters. They have had productive discussions with stakeholders and they've supported those changes in the Get Metrics to help address these issues.

ACCC noted that they will be shortly welcoming a new General Manager to lead their compliance, enforcement and exemption teams. Lauren White will start in 2 weeks' time and joins them from their Consumer Product and Safety area. The remaining regulatory guidance and future frameworks teams will continue to be led by David Jones.

ACCC noted that they have recently written to energy data holders to communicate the ACCC's expectations about ensuring compliance with the CDR rules and standard to improve energy consumer outcomes. This includes having clear and easy to find information about the CDR and training frontline staff to respond to relevant queries. The regulatory teams are also analysing the latest of the biannual reports under the rule 9.4 reporting requirements.

ACCC noted that in early July they launched the CDR developer portal, the purpose of which is to provide additional tools to support participants understand the ecosystem's technical requirements.

ACCC noted that last month they migrated their core systems and supporting infrastructure to a more secure and flexible cloud-based solution. The hyper care period has now passed with only minor issues which have been addressed. They thank the participants for their patience during the necessary outage for that change.

ACCC noted that last week they retired a number of the superseded API endpoint versions which has been fairly seamless so far and they will continue to monitor.

ACCC noted that there have been a dozen new software products activated since the last meeting, and removed four. There has also been a new ADR accredited and onboarded, which is the first energy use case data recipient and an exciting development.

Meeting Schedule

The Chair advised that the next meeting would be held remotely on Wednesday 8 November 2023 from 10am to 12pm.

Other Business

No other business was raised.

Closing and Next Steps

The Chair thanked the DSAC Members and Observers for attending the meeting.

The Chair again thanked Greg Magill from Westpac for his DSAC membership and wished him the best in his new role.

Meeting closed at 12:02