Consumer Data Right

Data Standards Advisory Committee

Minutes of the Meeting

Date: *Wednesday 12 October 2022*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Committee Meeting # 47*

Attendees

Committee Members

Andrew Stevens, Data Standards Chair	Chandni Gupta, CPRC
Luke Barlow, AEMO	Rob Hale, Independent
Damir Cuca, Basiq	D'Arcy Mullamphy, Adatree
Chris Ellis, Finder	Lisa Schutz, Verifier
Prabash Galagedara, Telstra	Aakash Sembey, Origin Energy
Peter Giles, CHOICE	Stuart Stoyan, Fintech Adviser
Melinda Green, Energy Australia	

Observers

Barry Thomas, DSB	Vaughn Cotton, ACCC
James Bligh, DSB	Andre Castaldi, OAIC
Ruth Boughen, DSB	Elaine Loh, OAIC
Rob Hanson, DSB	Bart Hoyle, Treasury
Terri McLachlan, DSB	Emily Martin, Treasury
Michael Palmyre, DSB	Kate O'Rourke, Treasury
Mark Verstege, DSB	Kate Penney, Treasury
Paul Franklin, ACCC	

Apologies

Jason Hair, Westpac	Tony Thrassis, Frollo
Zipporah Szalay, ANZ	Glenn Waterson, AGL

Chair Introduction

The Data Standards Chair (**Chair**) opened the meeting and thanked all committee members and observers for attending meeting # 47.

The Chair acknowledged the traditional owners of the lands upon which they met. He acknowledged their custodianship of the lands and paid respect to their elders, past, present and those emerging. He joined the meeting from Cammeraygal lands.

The Chair noted that it had been another busy month for the DSB team and they had a number of Decision Proposals and Noting Papers currently open for feedback.

The Chair noted that this was the last meeting before he refreshed the Data Standards Advisory Committee (**DSAC**); noting there would be some changes due to the increasing involvement in energy and in the not too distance horizon, the inclusion of telco. The Chair asked in the first instance, if anyone thought that it was time to retire from the committee, to let him know so he can incorporate this into the refresh process.

ACTION: Committee members to advise the DSB if they would like to retire from the committee as part of the refresh.

The Chair noted that Jason Hair (Westpac), Zipporah Szalay (ANZ), Tony Thrassis (Frollo) and Glenn Waterson (AGL) were apologies for this meeting.

Minutes

Minutes

The Chair thanked the DSAC Members for their comments, and last-minute feedback on the Minutes from the 14 September 2022 Advisory Committee meeting. The Minutes were formally accepted.

Action Items

The Chair noted that in regard to the outstanding Action Item for Westpac around whether the DSB could participate in the regular meetings with the bank's fraud teams.

The Chair noted Westpac had advised that whilst there were no formal intra-bank fraud and security sessions that they participated in, some other useful sources of information and/or organisations were Scamwatch, ID Care, Australian Cyber Security Centre, and the Fraud in Banking Forum which were coordinated by the Australian Payments Network.

The Chair noted that the DSB would re-consider how they may engage with banks in relation to cyber security, fraud and breach situations in the heightened environment post the Optus breach.

ACTION: DSB to consider how they would engage with banks in relation to cyber security, fraud and breach situations.

The Chair noted that this meeting was scheduled to be held in person in Melbourne but due to the limited number of members who could attend in person, the Chair meeting reverted to a virtual meeting.

Working Group Update

A summary of progress since the last DSAC meeting on the Working Groups was provided and these DSAC Papers were taken as read.

Technical Working Group Update

The update was provided on the Technical Working Group by James Bligh as follows:

The DSB noted that one member asked for an update on an issue related to the Standards ([Issue # 513 - Specify if an Account is a Joint account in the API Response)](). The DSB had moved this into Maintenance Iteration # 13 (**MI**) and stated it would be addressed through the MI process.

The DSB noted that with the implementations that were occurring, they were getting consistent feedback that participants were being overloaded with consultations and they did not have the bandwidth. But the DSB said they had also received lots of requests for new consultations from the community. The DSB noted that they have the capacity to do more consultations but they are cognizant of the community's bandwidth.

For example the DSB have had issues raised about Non-functional Requirements (**NFRs**) by both data holders (**DHs**) and accredited data recipients (**ADRs**). DHs had asked the DSB to review the NFRs to lower them and the ADRs are specifically asking for them to be raised in certain situations.

The DSB said they needed to consult on those objectives but at the same time they said they had the implementations in energy and banking and they said the community didn't appear to have the capacity to do further consultations.

One member asked for an update on the planning work for Action Initiation (**AI**) and whether there are any planned Workshops or Noting Papers in motion?

The DSB responded that were in motion, but it has not happened for the reasons mentioned above.

The member then asked, how do we prioritise and work through the competing priorities?

The DSB noted that this was their biggest challenges as topics like telco, AI, fixing NFRs and security are all priority number one. The DSB then welcomed feedback and guidance from the DSAC on topics they should tackle first.

ACTION: DSAC members to provide feedback and guidance on topics that should be consulted on and the prioritisation

The Chair noted that this group could provide input into prioritisation but the decision is ultimately made by the Minister.

TSY noted that they too were grappling with the tension between consultation overload and progress, and welcomed input from the DSAC.

One member noted that they had a high priority issue with the Transactions Per Second (**TPS**) limit and with some of their customers who had high volumes of users, but when they tried moving them across to Open Banking, they encountered constraints around TPS, which was a showstopper for them. The member said they were restrained by the number of requests they could make to specific DHs, which meant if their customer had a lot of users, that DHs would start rejecting their requests and the ADR would not be able to acquire the data.

The DSB said they had looked at this issue, and they could see its validity. They indicated this was an example of the prioritisation challenge they had. They said they would like to do a consultation on NFRs because this was something where a community trade-off was needed as this change would have a massive impact of the DHs.

The member said that conversely their existing screen scraping aggregators couldn't transition screen scraping customers onto the CDR, which was a massive issue for the regime and for the security of the customers that were still doing screen scraping.

Another member agreed that this put enormous pressure on DH's, particularly as there was a staggered implementation. They said that for those that are coming in late, and needed to have everything ready from day one, it was extremely hard and there was a risk that putting too much on DHs, also undermined what the CDR was trying to achieve with customers which can create gaps. They said this was a very high bar for DHs to initially meet.

The member asked if could the DSB provide a list of issues to the committee so they can provide feedback on their preferred priority?

ACTION: DSB to provide a list of issues for consultation to the committee for feedback on their preferred priority

One member noted that once there is AI, it will dramatically enhance the utility of the CDR; and that it will then drive more consumer activity, consumer uptake and more consumer participation, which will enhance and improve the CDR.

The member also asked that as the CDR moves to other sectors, what's the relative significance of adding additional sectors if we don't for example have banking or energy, right?

The DSB cautioned against seeing the sectors as distinct, because in banking the conversation is currently about issues of scale but in telco, they are taking about what data clusters mean, which is where banking was a couple of years ago, and therefore it is important to think about the sectors as waves of implementation and not necessary projects.

ACCC noted that it is a nice problem to have that the CDR is growing fast and it would be disappointing if we had to slow down the CDR to participants because of a restriction in usage.

The ACCC said that one of the challenges they would like the DSB to look at is not just how should the NFR change immediately, but how the CDR should move to a more sustainable mechanism of maintaining a forecast of growth, so that the CDR is not constantly bumping up against a hard cap.

ACCC noted that on the Performance Dashboard they publish the number of API Invocations and yesterday for example, they had 859,641 API invocations, which is a really large number per existing customer. They said they wondered if this was because there are a lot of automated requests for information that were not fulfilling an immediate customer request, and therefore not useful. They suggested that if this was the case, their removal might help solve the problem of the load on the DHs.

The Chair agreed that it would be useful to check this, and that there should be monitoring of a range of operational metrics.

The ACCC noted that they would be happy to discuss the problem with the major banks to see if the problem could be solved as quicky as possible.

One member suggested that there should be a staged NFR enhancement program that fixes the major primary brands and banking first.

The member also noted that the DSB's consultation process has tremendous value because it is interactive. They said they wondered whether the TSY rules consultations could perhaps be made more interactive, or at least have a couple of goes at it, which may result in a better outcome.

TSY noted that they have thought about this in terms of having a Design Paper that precedes the draft rules; offering as an example, the designation process starting with a Design Paper and then the Draft Rules, but noting their consultations are not a live interaction like the DSB.

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

A further update was provided on the CX Working Group by Michael Palmyre as follows:

The DSB noted that it has been another busy period with the publishing of a number of papers, v5 rules and AI which they have provided feedback on.

The DSB had left open the issue for Decision Proposal 267 on telco language standards now that the proposed v5 rules has been published for consultation. They said they were working toward the second version of that DP with the final round of consultation planned for November.

The DSB noted the first round of research on the CX of Authentication had concluded, which focused on the current 'Redirect with One Time Password' model. They said preparation was underway for the second round of research, which would focus on app-to-app authentication. They said research had commenced in August and would continue until the end of the year in order to cover several authentication approaches and iterations.

The DSB noted that two rounds of CX research had now been conducted for the consent review work. They said the first round focused on attitudes towards data sharing and a prototype of the current consent to collect and use flow, while the second round tested a simplified version of the consent flow. They said analysis was underway in order to assess how well these flows performed against key metrics for trustworthiness, informed consent, comprehensibility, and empowerment. They said a third round was being kicked-off, which was expected to iterate on the simplified flow tested in round two.

The DSB noted that by the end of the year, they would have reached around 300 research participants which was a good scale and included one-on-one research sessions, surveys and in-depth exploration with consumer participants. They said that including the authentication and telco research the number was closer to 500 consumers by the end of the year.

The DSB proposed to move the CX Guidelines Change Requests into the Maintenance Iteration and the Standards Maintenance Website because they received many requests to include these as part of the Maintenance Iteration. They said this would enable more exposure and a way to prioritise the backlog of CX Guidelines.

The DSB noted that the final Accessibility Report, and improvement plan, that was developed with PwC's Indigenous Consulting (PIC) and the Centre for Inclusive Design would be published soon. They said the report would be published on GitHub for community feedback, and that the DSB are developing their own responses to the report before consultation. The DSB noted that one of the recommendations was for an uplift to the accessibility standards and for them to be consistent with non-CDR obligations related to accessibility e.g. The Disability Discrimination Act 1992.

One member noted that in terms of authentication, in the telco sector there's a regulation that mandates two step verification, and they asked if the DSB was looking at that in their authentication journey. They also asked that in the wake of the recent cyber-attack if the DSB was considering any insights through that process.

The DSB noted that from a CX perspective, a lot of their work was based on community requests and security reviews of the authentication approach, which was articulated in both the CX and technical standards. They said their research looked at improved approaches on the existing standards and what they need to consider moving forward for the authentication uplift. They said their key foci were around security, consumer adoption, friction and the possibility of drop-offs and failures with respect to authentication.

The DSB noted that when it comes to authentication, they don't think a blanket approach for all sectors was appropriate, and a waterfall approach with app-to-app may be required, where if this was not available, a redirect with OTP could be used.

The DSB also noted that in regard to security and identity theft, the issues they've got with adopting app-to-app with CDR, which is the disadvantage they had over Open Banking Implementation Entity (**OBIE**) in the UK from a technical perspective, was because the CDR was cross sectoral, and not every sector has apps. They said, when they get into energy, the major retailers all have apps but adoption is very low and the long tail of retailers don't have apps.

The DSB noted that they would like to consult on this from a technical perspective as there are some things that they could do to address the security concerns addressed in the security review around the use of SME, text message and OTP, which had nothing to do with an app-to-app modality.

The DSB noted security was a big focus, and at the moment with "read only" even the security reviews have indicated that we have a current issue that they also flagged in the future was going to be more and more of a problem.

One member asked in regard to the accessibility work that had been done, had the DSB also considered linguistically diverse consumers as part of the ecosystem they're considering?

The DSB noted that they engaged [PwC's Indigenous Consulting](#) (PIC) and the [Centre for Inclusive Design](#) to do this work which included the technical interpretation of accessibility in relation to Web Content Accessibility Guidelines (**WCAG**), including the linguistical and digital issues that may result in barriers to adoption of CDR. They said that this had always been a consistent approach in the CX research.

The DSB noted that there are some other recommendations like considering inclusivity, accessibility and usability framework which they would look at more broadly.

The DSB noted that they would be seeking ways to engage with more consumers representatives and they would be reaching out to the Consumer Policy Research Centre (**CPRC**) in order to better understand the environment and to find better ways to interact with consumer representatives in their standard setting and potentially rule making processes.

One member noted that in terms of tracking and measuring, lots of resources were spent to convince consumers to use their services, and they were actively tracking every button click to understand where the drops off are and how to optimise the experience.

The member also noted that businesses were often provided multiple services and sometimes they needed multiple requests of consents that weren't directly related to the CDR. They asked whether

there has been any consideration or provision in service on how the CDR consent framework could provide some opportunity for other consents to be incorporated which are outside of the CDR program?

The DSB noted that from a CX perspective, and the work they've been doing on the consent review research, there are things that would preclude that from happening with the current Rules because the requirements effectively prohibited the bundling of consents, especially with non-CDR consents. They noted that this is not precluding or presupposing anything that might happen with CDR developments, but they saw AI as the way into some of those issues.

The member wanted to emphasise and acknowledge that no one will download an app just to use the CDR, and a value exchange needs to be considered. They said that if the CDR operated in a vacuum and pretended that these consents don't exist it would create a big disconnect and there would be a big drop off.

The DSB noted that their research confirmed with the Rules and requirements on bundling and going beyond this was a broader policy consideration.

TSY confirmed the wider policy considerations and issues, including protections attached to consents, are being considered as part of the work being done jointly with the DSB.

One member noted that there was a lack of visibility when the consent flow goes to the authorisation flow. They said there was a significant variance in the drop-off with different DHs and therefore the more information they could get to understand this and to implement good practice was important.

The member also noted that in terms of the possibility for consenting to other things in the same flow as the consent flow, they said that this needed to be addressed with AI because fundamentally if consumers were consenting to an action being taking on their behalf in CDR there also needed to be some information provided about what the action was going to be and how that could be addressed.

One member noted that the Statutory Review of the CDR raised this issue in Finding 2.2 around the concept of bundling and what might be needed to reduce the overhead. They said in terms of the maturation of the scheme, it would be good to explore to prescription versus principle approach again as implementations needed to understand the critical points around getting data and how to communicate consent.

The DSB noted that they had also been looking at the recommendation on bundling as it was a really important starting point. They said their CX research was looking at some of those prescriptive points, like actively selecting things that were essential for the provision of service and whether that made sense.

The DSB noted that they did some preliminary work around purpose-based consents and the idea of helping the data minimisation principle was in the line with CX of bundling and the different scopes. They said they had been looking to resurrect that conversation as it was going to be a contributing factor to AI.

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.

Issues Raised by Members

The Chair thanked all members who had tabled discussion items.

Presentation on "The Impact that the current approaches to ID have on CDR (and vice versa)" by Verifier

Lisa Schutz from Verifier presented an overview of the impact that the current approaches to ID have on CDR (and vice versa) as follows:

Schutz noted that Australia was at a watershed moment in data sharing and she wanted to highlight the two-way flow of things that were going on around the Optus hack and the related impacts and opportunities for the CDR.

Schutz noted that she has been a long-term participant in the CDR and has been on the DSAC since inception. Verifier has built and operates a Privacy Principle 12 "consent + search" network using a search-based model of consent which is used for proof of income in Australia and that there was an opportunity to use the CDR to protect customers and the system with the addition of a search-based consent pattern.

Schutz noted that the recent Optus hack could have happened to a number of organisations as it was a systemic issue. There was an opportunity for consented data sharing and to give customers and the system a sense of control back quite quickly.

Schutz noted that the top priority was to stop the risk of ID theft, followed closely by giving consumers back control of their digital selves. This was where she believed the CDR had a considerable role to play by enabling customers to remediate their ID without huge time and cost, and to ensure that people on that list are not barred effectively from all automated processes.

Schutz noted that as a third step, there was also a critical role for the DSAC to participate in a review of the ID reliance system and to review the overall approach to establishing identity online in Australia. This was not about digital ID but how as a system we rely on ID.

One member noted they supported Verifier and noted that there was no one playing a critical role in the economy to mitigate the system costs of identity theft and the DSAC had a huge role to play. They said as a consumer this was a burning platform for them.

The Chair noted that this presentation would be especially relevant to TSY and OAIC who were involved in interdepartmental committees in response to the Optus hack, and that the Verifier proposal could be fed into those considerations, subject to input from the DSAC discussion.

Schutz noted the Optus hack file sharing changes to the Telecommunications Regs that had been proposed and implemented, with many ordinary Australian's going about their business were now on a "watchlist". Some issues with watchlist file sharing are:

- It may upset customers on the list that their data was moving around without their consent and being proliferated not contained
- Why only Australian Prudential Regulation Authority (**APRA**) regulated parties? There were ID relying parties everywhere in the economy
- Once on the watchlist – there was a significant maintenance problem. How would you get off the list if you had changed credential(s) or solved the problem?

- Even if you solved that and found a way to update the watchlist at its source, copies of the watchlist may not be in sync
- Needed to find non-ID document ways to check that person was real and not fake if they hit the watchlist

Schutz noted that sharing watchlists perpetuates the problem. Some issues where consumers are impacted by one data breach, were then on a watchlist shared with the identity ecosystem, and they were then barred from most automated processes, even when the consumer proved who they were, because relying parties may not have the latest watchlist; and what if the relying parties had a data breach of their own?

Schutz noted that consent driven data-sharing reduced the problem. She proposed to leave the data at source (i.e. whoever is breached) and when the consumer was asked whether they would like to check their name and details against the watchlist, they were referred and they would need to prove themselves to the satisfaction of the relying party. In this scenario as there was only one watchlist file, the new information would be updated to either take them off the list or adjust the list to incorporate a second factor that was in their control etc. But the consumer was in control of sharing their data throughout. That would be achieved if such watchlists were designated under the CDR.

To fix the other issue, of finding "out of wallet" data to mitigate the risk now in the system, Schutz suggested that there was a set of data that had not been impacted by that breach (and those like it) which was proof of employment information which could be sourced from single touch payroll (STP) and Superstream data, which could also be released in a consent driven way – using the same search pattern in CDR.

The Chair asked for clarification on whether the company that had the data breach would be the DH of the watchlist and that there was only one version of it? He asked if all referrals, consents and updates would be on one version, not multiple versions held by multiple APRA entities?

Schutz noted that what she was proposing was where there was a significant data breach, that only the watchlist related to the breach would be designated. They were not proposing that CDR take over identity verification or get involved in any way in the document verification service or any of the current ID reliance processes. What they were proposing was a complement to the existing ID reliance system, as an additional piece of data available in a consent driven way if an organisation wanted to use the watchlist. This would be the mechanism for these organisations to add that to their existing processes. This would be additive to the Document Verification Service (DVS) which was the primary mechanism organisations relied on for ID verification.

Schutz noted that in the proposed approach, the difference is that the Oauth style network is replaced with Consent and Search Function which can be fulfilled by intermediaries or ACCC.

The DSB noted that something like this would need to go through designation which takes time and possibility new rules and legislation. They asked had Verifier thought about whether this could be done using the CDR infrastructure framework on a voluntary basis and what that could potentially look like?

Schutz noted that the watchlist was trivial in that it was a flat file. For the Consent and Search API via search, Verifier (or others) could work with the ACCC because they had a search algorithm and the accreditation process for the ADRs that were in place. They said they didn't think this needed to be designated because if the DH wanted this to complement the CDR and be available to accredited persons and were willing to work with Verifier (or others) this could be implemented in a month.

Schutz noted that Australia was at a watershed moment around trust in the digital economy, and we as a group have an opportunity in time to work with the principles of CDR to effect better outcomes, in a way that doesn't require designation. They noted that when a DH really wants to get things done, they can do things in an emergent (Privacy Act) way.

Schutz noted in terms of updating initiator (to initiate remediation of list), ADRs were unlikely to want to share data without some level of designation. They said this might, however, be a bridge too far until it being designated.

The DSB noted that one of the strengths of the CDR was that it is completely distributed. They said that apart from the Register, there's no central infrastructure to attack, such as centralised databases etc. They said this proposal did present a central service however which was very different to what has been done to date. They said this potentially created weaknesses because a central service could be a weak point both operationally and from a data breach perspective.

Schutz agreed that the one single point of weakness in the current system is the ACCC Register, but they would point out that in their proposal the data remains at rest and the search API doesn't have to be one entity. She said multiple intermediaries could do the search process and the data could be deidentified so there wasn't a central repository.

The DSB asked if they have thought about whether it could be done without a central (or multiple) services because they thought that was worth a conversation.

The DSB also noted that one of the things about a service like this was that if everyone starts depending on it for identity provision or providing access to services that were essentially giving consent, it ceases to be optional which was a concern.

Schutz noted that by promulgating the Optus related watchlist, that at least 2.1 million people were effectively being barred from automotive processes from the start. She said they would need to work out how to make this consent driven data sharing work for people, which is the lesser of the two evils – no automation or checking to see if you are on a watchlist being part of the process. If you do not consent, you have to go to a more manual process.

One member noted that there was no doubt that the CDR, within the framework and the service it provided, helped contribute to a solution in terms of prevention and particularly from an identity perspective. They wanted to know the view of the CDR's responsibility from an ID perspective and said it would be good to have further conversations about it.

The Chair noted that his understanding was that the organisation with the data is the DH, and they should therefore maintain the watchlist. He said the data would already be comprised, but he wondered if the consumer would trust the DH to manage the watchlist having not secured the data initially.

Schutz proposed that the first thing needed was a consent driven Watchlist which could be done either via the CDR or as a voluntary complement to the CDR (outside of the CDR regulations) that is accessible to accredited persons. She said designation would take longer, but the principles of the CDR, the requirements of the DHs and the accreditation of the recipients were already there and could be used voluntarily without being designated.

For the out of wallet data, Schutz suggested that designation was likely to be necessary. They suggested that STP and Superstream data in the hands of the gateway operators of Superstream is immediately available with a search pattern, as the APIs are already in place at least for a portion of

the DHs, but access was restricted because Equifax is claiming in the market that it had locked up the search API capability for STP 2.0 by contracting directly, on an exclusive basis, with a number of the bigger STP 2.0 DHs. They suggested that Treasury might want to confirm with the DHs directly what the situation is, as they did not know for sure.

OAIC noted that in regard to the Watchlist file sharing process, and not downplaying the application of CDR as a remedial step in relation to these sorts of issues, they had looked at this in a very privacy protective approach to the way that work been stood up under the legislation. The OAIC said they had an ongoing monitoring role, along with the ACCC in relation to information in the hands of the APRA entities.

The Chair thanked Schutz for her presentation and noted that he understood the direction of their work but noted some of the practicalities needed to be progressed and fine-tuned so it could be validly considered.

Treasury Update

Kate O'Rourke, First Assistant Secretary CDR Division, TSY provided an update as follows:

In response to an earlier question on the Government's strategy with respect to CDR, TSY confirmed there is a commitment to maintaining the momentum of rollout of the CDR, both with respect to developing action initiation, and rolling out to new sectors.

TSY noted that the CDR Exposure draft legislation to enable AI had been published for consultation, which was followed on with a forum on 11 October. They said this was their first step in the development of a regulatory framework, and would then be followed by Rules, declarations and Standards.

TSY noted that the Statutory Review of the CDR was tabled on the 29 September, which was out of session in Parliament. They noted that one of the recommendations was to undertake a security assessment of the system as a whole, which was something they have already started and is an important issue.

TSY noted that they had some Rules out for consultation that extended the CDR to the telco sector, as well as operational enhancements, with the most important one being the proposal of a business consumer disclosure consent. This rule package also has proposed changes to the rules on reciprocity and the length of consents.

TSY noted that in regard to Rules, there was also an opportunity for stakeholders to feed suggestions on Rules changes to be considered in the future.

TSY noted that there had also been a lot of work related to the government response on the Optus breach which they had been involved in.

ACCC Update

Paul Franklin, Executive General Manager ACCC CDR Division provided an update as follows:

The ACCC noted that two of the initial energy DHs had completed conformance testing in preparation for activation as DHs. They said they would work closely with them, and the Australian Energy Market Operator (AEMO), with a view of activating them no later than 15 November in order to allow for production verification.

ACCC noted that across all active DHs the average availability in September was 99.7% and in the first 11 days of October it has been 99.88% which was above the requirement of 99.5% availability and this continued to move upwards.

The ACCC said they were continuing to see a steady stream of accreditation requests but also a very significant number of representative arrangements being implemented. They said they had 45 representatives active on top of the 23 active ADRs.

ACCC said they were now publishing the number of API calls and were also looking towards publishing the number of ongoing consents in place by the end of the year.

One member noted the recent deadline for the commencement of joint accounts for non-major banks and asked if they could have some visibility about how many of the DHs are meeting their requirements. They noted that one of the providers had announced that they would not be meeting their joint account deadlines until February 2023, and they were also not releasing or didn't have account details API available for phase one or two products which was quite a significant concern as those were obligations they'd had for some time.

ACCC noted that they published a rectification schedule where there were known compliance gaps. They said their experience with previous deadlines was that it was not always clear on who was going to make it or not and their aim was to get information published ASAP. They were also looking at the rectification schedule in light of recent feedback to see if additional information could be provided.

ACCC noted that they didn't comment on any compliance and enforcement issues until they had reached a resolution, but there was useful operational data that could be provided and should be provided in relation to this.

ACCC noted that the Incident Management Working Group had discussed potential improvements to the incident management process and at the next meeting they would be looking at a proposal for service level objectives.

ACCC noted that in terms of data quality there was a clear gap in the information available to both qualitative and quantify the data quality and they needed more information to be able to better understand exactly where the issues existed and how frequently they were occurring.

Meeting Schedule

The Chair advised that the next meeting will be held remotely on Wednesday 9 November 2022 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.

Meeting closed at 12:05