FinTech Australia

Screen scraping: Policy and regulatory implications

Submission
October 2023

About this Submission

This document was created by FinTech Australia in consultation with its members. In developing this Submission, interested members participated in roundtables and individual meetings to discuss key issues and provided feedback to inform our response to Treasury's discussion paper.

We acknowledge the support and contribution of K&L Gates to the development of this submission.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech sector, representing over 420 fintech companies and startups across Australia. As part of this, we advocate on behalf of a range of consumer data right (**CDR**) participants as well as fintechs spanning payments, consumer and SME lending space, crypto and blockchain, wealthtech and neobanking, regtech and insurtech. Our members also include data aggregators and fintechs which use screen scraping.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

FinTech Australia would like to recognise the support of our Policy Partners, who assist in the development of our submissions:

- Allens
- Cornwalls;
- DLA Piper;
- Gadens;
- Hamilton Locke;
- King & Wood Mallesons; and
- K&L Gates.

Executive Summary

Fintech Australia recognises the great opportunities that the Consumer Data Right (CDR) presents. We are excited by the potential for CDR to support the rapidly developing, data-driven economy here in Australia. Despite this, our members report use of screen scraping is still widespread and transition to CDR will be difficult in the short term without urgent changes to the CDR framework to support transition.

FinTech Australia supports in principle the phasing out of screen scraping, consistent with the 'viable alternative' precondition set out in the Statutory Review of the CDR. Members are generally supportive of encouraging a graduated transition to CDR in circumstances where CDR is available and a viable alternative. However, some members also suggest screen scraping should remain available as a 'back-up' option until CDR data quality, derived data usage restrictions and consent flow issues are fully resolved.

For CDR to be a viable alternative to screen scraping, it must have at least equivalent capabilities with respect to the availability of data, quality of data, ability to use the data, connectivity and ease of use for consumers. Specifically, data holders should be mandated to offer online authentication methods for granting consents. The digitalisation of the consent process would significantly streamline data-sharing activities, making it easier for consumers and small businesses to manage their consents in real-time.

Essential to any phase out will be clear timeframes and deadlines. Those currently reliant on screen scraping and the data recipients which will help them transition to CDR need certainty. This need for certainty applies not only to the timing of a 'ban' but also the improvements to the CDR framework required, from a technical, regulatory and consumer perspective, to support this transition.

We propose that clear benchmarks are introduced to enable regulators to track progress of data holders towards prescribed goals and that a complete ban on screen scraping is not implemented until these data holder benchmarks are achieved and after a clearly defined transition period.

Our members are also of the view that a key prerequisite to CDR becoming a viable alternative to screen scraping will be enforcement by regulators on the actions of data holders, to ensure they are providing quality data through the CDR APIs. Trust and confidence in CDR data is fundamental to it being accepted as a viable alternative by those currently reliant on screen scraping.

1. How is screen scraping currently used?

1.1 Screen scraping practices

Screen scraping remains commonly used by a range of fintechs, particularly those in the lending space and primarily in relation to banking data. Other data captured could include non-bank lending, superannuation, insurance and government (MyGov) data.

FinTech Australia members report using screen scraping practices in various ways, including but not limited to:

- gathering supporting financial and identity documents in order to onboard finance and other applications;
- obtaining customers' Centrelink Income Statements through myGov;
- obtaining identity details;
- verifying bank accounts;
- obtaining Australian Tax Office Notices of Assessment;
- obtaining PDF copies of online banking statements;
- obtaining transaction data from Banks;
- validating of financial data;
- enabling financial/wealth management services;
- categorising income and expenses;
- supporting transaction monitoring for compliance with AML/CTF obligations;
- confirming consumers meet eligibility criteria for products (i.e. in compliance with Target Market Determinations);
- conducting serviceability assessments for credit decisioning; and
- obtaining superannuation investment data.

1.2 Steps taken by consumers, screen scraping service providers and businesses in the screen scraping process

The screen scraping process typically involves a screen scraping service provider (data aggregator) providing API services and an interface which a client can integrate within their application. These arrangements allow for a high degree of flexibility and control over the user experience and UI flow. This means the steps and interface can vary greatly depending on the business model and use case, however, the steps involved would typically include:

- A list of institutions the screen scraping service provider supports;
- An authentication form to capture login details required to source data; and
- Access to the terms and conditions for how data will be used and handled.

There is no mandatory consent process for screen scraping. However, our members note that many of the consent processes used by screen scraping providers contain many of the elements of the consent processes used in CDR. The main exception is an active hand over of the customer to the bank for the authentication component.

In particular, the steps often include the following elements:

a) Consent protocols

Many of our members initiate the data retrieval process at the request of their clients, who require specific data from end users. As part of the consent process, the end users are typically provided with information about what data is to be obtained and what the data is to be used for. The end users will provide an informed use-consent based on detailed information. Consent is expressly obtained, rather than implied, in compliance with Australian regulations.

Some of our members may not include all of the information on the "front screen". The extensive explanation of data use and storage will be provided through a hyperlink that users can click through to review the terms and conditions. Despite this, the high level disclosure is clear on the front screen. Our members use consent protocols that contain an active opt-in consent.

The configuration of consent will differ and depend upon the clients' needs for their specific use cases. Our members view this as a significant benefit of screen scraping in allowing the consent process to be bespoke and tailored to enhance user experience and increase the change of completion. One of the current barriers to CDR becoming a viable alternative to screen scraping is that the consent flows are still relatively complex (and, in some cases, require manual interactions), which is reported by some to result in lower conversion rates. We acknowledge these issues are being considered and addressed through Treasury and the DSB's ongoing CDR Consent Review consultation. FinTechAustralia provided feedback separately to that consultation.

b) Limited duration of consent

The duration of consent obtained by our members may be one-off or ongoing. Typically, our members would seek consent for no longer than one year.

The duration of the consent will depend upon the required use case. For some of our members, where users agree to provide ongoing consent, they will get a link to refresh their consents on their own dashboard as well as information about whom they have provided data to, when the consent expires and offers them the opportunity to withdraw consent immediately.

2. What are the risks of screen scraping?

2.1 Risks to consumers from sharing their login details through screen scraping

Members did not identify additional risks to consumers from sharing their details through screen scraping to those identified in the paper.

Views about the significance of these risks and the appropriate regulatory approach varied.

Members generally acknowledge that while there may be concerns about data security, these have not translated into widespread consumer harm or loss from compromised data based on members' experience.

Most of these members supported the CDR being supported to become a viable and secure alternative for data sharing, and considered this would drive consumers and businesses to transition to CDR, obviating the need for specific regulatory intervention. In relation to the risks identified in the paper, these members provided the following observations:

a) Context

Several members raised that "disclosing" login details is not unique to screen scraping and often occurs through online password managers and in-browser password storage tools.

For businesses which make use of screen scraping data, they would typically receive the screen scraping data from a screen scraping service provider (aggregator). While the end user would need to provide their login details to the screen scraping service provider, the business ultimately accessing the screen scraping data would never access the login details themselves. This ensures that the login details are controlled by those with the necessary security systems to manage them.

b) Screen Scraping as a mature technology

Digital Data capture has been used for at least 20 years and is a reasonably mature technology. Some members believe that providing the ability to secure access credentials is critical to continued participation in the industry and most businesses have adequate security to manage the risks.

c) Security infrastructure

Many of our members have multiple layers of security around username and password credentials and suggest that even where a breach were to occur, actually obtaining someone's credentials is highly unlikely.

They also noted screen scraping providers implement measures and data security standards to mitigate risks arising from the sharing of login details. However, much of this risk sits with the screen scraping providers and it is incumbent on them to prioritise security and implement appropriate controls.

Some members have also started applying the CDR framework's requirements to scraping services. This can ensure data is handled in a more consistently secure manner regardless of how the data is acquired.

Concerns about latent risks

In contrast, other members raised serious concerns about these risks and considered them significant, even if currently latent. These concerns relate to screen scraping not being specifically regulated and the potential cyber security risks for screen scraping providers and potential for them to be a 'honey pot' of

login details. They also flagged the risks associated with breaching bank account terms which prohibit giving banking passwords to third parties and the resultant liability issues for associated unauthorised transactions. Concerns were also raised about the potential for further and ongoing use of scraped data which generates income through additional unregulated data sharing and that the only way to address these risks is through a ban.

These members also flagged that compared to the CDR framework, there is a lack of transparency in relation to the sharing of scraped data with third parties. This could result in a relatively greater risk of misuse and uncontrolled data sharing with additional third-party organisations.

2.2 Circumstances where screen scraping capabilities have been blocked

Some of our members have experienced their use of screen scraping being blocked by banks. This occurred when a bank was transitioning to the CDR regime and determined to fully block screen scraping.

For ongoing services, members report the increasing use of MFA for login has blocked ongoing data collection through screen scraping.

Members report banks may also use 'bot detecting' technology to pick up bad actors, and at times, the banks' technology will detect other screen scraping users and block their use.

Some members hold concerns that there may be a soft ban on screen scraping implemented by banks prior to the Government commencing a formal ban. They consider there is a risk that banks may elect to block screen scraping which will have a large impact on businesses that rely on screen scraping and consumers that use these services.

Our members are aware that one of the major banks has written to customers and has warned them directly about the risks of screen scraping. Members are concerned that this may be anti-competitive, disruptive and lead to banks asserting that CDR is viable now, in effect resulting in a soft ban. Certainty about the phasing and timing of any ban, without pre-emptive action by banks, is essential to ensuring a smooth transition and minimal disruption to end users and consumers.

2.3 How organisations and entities are managing the risks associated with screen scraping

As discussed previously, our members report having robust security systems/processes in place to reduce risks for consumers. This includes but is not limited to having comprehensive disclosures around consent for use for customers, providing opportunities for customers to opt out of consent after it has been given and ensuring login information is stored appropriately.

We have not exhaustively listed these measures, but many FinTech Australia members will make individual submissions outlining their governance and security controls.

3. The Consumer Data Right

3.1 What are your views on the comparability of screen scraping and the CDR?

Our members note that broadly, screen scraping typically involves simpler journeys for users and lower costs of compliance than CDR.

Our members consider that there are gaps in the capabilities available through CDR when compared to screen scraping in addition to concerns with the quality of data available through CDR. Additionally, there are differences in the default customers that are available and the processes which they are required to follow.

a) Product differences

The types of products that can be used within the CDR framework differ to that which can be used in conjunction with screen scraping. CDR only applies to a subset of banking products, whereas screen scraping is used for a much wider range of products and datasets.

For screen scraping, all accounts and transactions are accessible when a connection is established. This contrasts with CDR where consumers choose the accounts to share. While this gives consumers more control, members report it limits CDR's suitability for certain use cases. Rather than having a consumer's full financial picture, as is available with screen scraping, certain accounts can be obscured under the current CDR framework. This limits CDR's usefulness in performing use cases like affordability assessments and meeting responsible

lending obligations. Members suggest greater flexibility in how ADRs can request access to the accounts needed to use their services could bridge the gap between screen scraping and CDR.

b) Data accessibility differences

A concern of our members is the fact that data designated in the data standards as "optional " may not in practice be provided by the bank, even when it is available. This is not consistent with the obligations on data holders, but is occurring in practice. Data recipients are unable to "see" what data is available practically and need to rely on the assumption that banks have provided all of the "optional" CDR data which was available. However, members acknowledge this is likely more of a compliance and enforcement issue rather than a deficiency in the framework itself. These issues also vary depending on the individual data holder.

Members also report screen scraping sometimes providing additional data points not available under CDR, such as date of birth and a running balance.

CDR can provide richer and more structured datasets compared to screen scraping. The standardisation CDR mandates means data can be more comprehensive and overcomes the variability of screen scraping, which can vary greatly depending on the data visible on the front end for each institution. For example, Merchant Category Codes are also available under CDR which provides better classification of expenses. This can assist lenders and financial management service providers to understand consumer expenditure patterns.

However, other members report data aggregators using screen scraping can provide rich industry segment data sharing which is well established and not necessarily yet available under CDR. Scraping has had years of developing transaction categorisation models, codes and formulas for particular use cases like instant loan decisioning which can, for example, be easily shared with intermediary acquisition channels. Members in the lending space interested in switching to CDR cite this as a key obstacle to adoption for them and a range of other fintechs in mass adoption segments like wealth management, insurance and accounting.

CDR also provides access to product reference data. Although members report some issues and inconsistencies with this data, they acknowledge it can be more reliable than scraping for comparing metadata like fees and interest rates for

specific products. This information plays a crucial role in powering comparison and switching/retention use cases.

c) Data quality

Many of our members note there are distinct differences in the data quality currently available through CDR when compared to that which is available via screen scraping. Currently the data obtained through screen scraping is regarded by many members to be of a greater quality and reliability than what is available through CDR. However, other members, including intermediaries, find authenticated CDR data to be better quality and richer data. They also note it is important to distinguish authenticated data from product reference data, which is new and faces different quality issues.

Our members are concerned that there are no data quality controls currently through CDR and that the framework lacks rules that provide any protection with respect to data quality.

Furthermore, data quality does not appear to have been an enforcement focus. We consider that this is necessary in order to drive strict compliance with the data standards. Members suggest extending the conformance testing for data holders to include testing of data quality. Although members recognize the origin of data quality issues might be inadvertent or unintentional, there is currently little incentive for data holders to invest in rectifying them.

Trust and confidence in the CDR are essential, not just for individual consumers but also the businesses which will drive use cases and uptake by shifting from screen scraping. The perception of data quality and reliability issues, relative to screen scraping, limits its success and must be addressed for it to be embraced as a viable alternative. This could be through a combination of education, improvements by data holders and a stronger compliance focus.

d) Data use

Our members are concerned about the restrictions on use that are inherent in CDR data. In particular, any data obtained via the CDR APIs, as well as any data which is "derived" from that data, retains its character as CDR Data and is subject to a range of additional privacy protections and restrictions. These protections and restrictions apply indefinitely and cannot be overcome by informed client consent (except in limited circumstances for business consumers, insight or trusted advisor disclosures). This presents a significant barrier to a broader

uptake of CDR, as the use of such data is more heavily restricted than data obtained in any other way.

In addition to use restrictions, our members remain concerned also about issues with being able to disclose CDR data.

While business consumer disclosure consent changes were designed to address some of these issues, they do not do so universally, and challenges remain. For example, blockchain solutions currently cannot meet CDR data deletion requirements. Additionally, no banks are presently enabling the processing of payments derived from CDR data. Some use cases, such as setting up payment instructions with third-party payment providers, face limitations under CDR due to data sharing restrictions.

Another example is financial management platforms that enable consumers to install plugins or addons and grant access to their advisers. Under CDR, the 'use' restrictions make this challenging without obtaining additional consents or having the addon become accredited. Screen scraping, on the other hand, does not impose such constraints, allowing for a broader range of use cases. In our view, until it is compatible with a wide range of platforms and financial tools to ensure seamless data integration, the CDR cannot serve as a viable alternative to screen scraping.

3.2 Restrictions related to data use and disclosure under the CDR

Our members regard that there are inherent challenges in comparing CDR Data with screen scraping data; it is not a straightforward task.

a) Derived data

Our members note a particular concern with the challenge of using derived data. The effect of the CDR data and derived data definitions is that wherever CDR data goes, it must have CDR data protections attached. Members report this contrasts with the approach taken in the UK in relation to Open Banking where there are fewer restrictions on data use.

Regarding derived data, our members have some concerns that the mandated use of CDR data could mean that proprietary datasets and machine learning or AI models, that have been developed outside of CDR may ‘become’ CDR data. This is as any combination or derivation of CDR data will become derived data. This would be unworkable given the consumer consent requirements and

significant use and disclosure restrictions. This would severely limit the operation of machine learning and AI models, ultimately to the likely detriment of the customer. Striking a better balance between privacy and utility is a key issue and CDR data's value and usability must be more comparable with scraped data for it to be recognised as a viable alternative.

b) User experience

The user experience for screen scraping is typically simpler and easier to use when accessing a data holder's interface. The experience is more 'seamless' and stays within a single screen when consumers provide their login. This contrasts with the experience under CDR, which redirects consumers to the data holder's portal to authenticate, consent, select accounts and agree to terms before being redirected back. Members report this can result in drop-off/abandonment due to the disjointed flow and multiple steps involved.

In relation to user experience, screen scraping is generally considered more consistent, usable/native and less reliant on data holders to provide a good user interface. Although we understand these issues are currently being considered as part of the ongoing CDR Consent Review, CX should be continuously evaluated and ways to encourage data holders to improve user engagement, in collaboration with ADRs, should be considered.

c) Complex business structures

Businesses with complex structures and data sharing arrangements find screen scraping easier to implement. Where there are related parties and distribution channels, members report businesses have difficulty navigating the CDR's accreditation model. Data sharing with third parties, often operating under the same software service or AFSL licence, is inherent to some business models and the CDR's restrictions mean screen scraping is easier to use. Members suggest there is a role for more guidance and education for businesses about accreditation options and the overall benefits of adopting CDR.

d) Exceptions from the CDR framework

Members have also raised concerns about the exceptions for certain account types, which means particular use cases which are possible through screen scraping are not available under CDR. Examples provided include inconsistent treatment of corporate trust accounts by different data holders, with some not providing access depending on how the account was set up or if internet banking

is available. This inconsistency and uncertainty limits businesses with 'CDR ready' data use cases being able to confidently switch from screen scraping to CDR data.

e) Business banking

The sharing of business banking data has been raised by members as particularly complex via CDR. Businesses must go through a process which can include filling out paper forms, obtaining signatures of authorised people and waiting for a manual approval process. This contrasts with screen scraping, whereby the business can provide login details to a screen scraping provider which instantly collects data.

3.3 Revising the CDR framework to make it a more viable alternative to screen scraping

Members have suggested several key revisions to the CDR framework that would make it a more viable alternative to screen scraping:

- **Data integrity**: Guarantee the accurate and timely transfer of data, ensuring that all data elements are consistently up-to-date and reliable.
- **Online authentication methods**: Mandate that all data holders offer online authentication methods for consents, thereby eliminating the need for outdated and inefficient paper-based processes.
- **Coverage and account types**: Ensure the CDR framework supports the availability and coverage of all financial account types essential for the effective operation of small businesses, including but not limited to transaction accounts, credit accounts, and investment accounts.
- **Interoperability**: Ensure the CDR framework compatible with a wide range of platforms and financial tools to facilitate seamless data integration.
- **Enhanced flexibility**: Revise the CDR framework to allow for more flexible data sharing options, akin to screen scraping. This would accommodate a broader range of use cases, including third-party payment setups and plugin/addon installations. Some members also suggest extending the Business Consumer Disclosure Consent treatment to a broader ange of consumers.

- **Improved awareness**: Ensure data holders are raising awareness with and educating consumer facing staff about the CDR framework so they understand it and can support their customers to engage with it. Broader consumer and business education campaigns, as raised in the CDR Statutory Review, are also supported.
- **More timely rectification and minimising disruption**: Address delayed responses to tickets raised by ADRs with data holders and delays to issues on the rectification schedule. Disruptions to the flow of data undermine confidence and usability of the CDR for businesses moving away from screen scraping. This could also involve more streamlined processes for recipients engaging with the ACCC Registry.
- **Certainty about future direction**: Provide clearer timelines for future sectoral expansions, functional changes (e.g. action initiation) and messaging about next steps. Sudden 'pauses' and ambiguous assessment processes cause confusion about the rollout and uncertainty about the future of CDR and investing in implementing it as an alternative to screen scraping.

By addressing these points, we believe the CDR framework can become a more attractive and viable alternative to screen scraping, thereby fostering innovation and consumer choice, confidence and control.

3.4 The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative.

How should the Government determine if the CDR is a viable alternative?

For the Government to be satisfied the CDR is a viable alternative to screen scraping, we recommend the establishment of a robust definition and framework for what constitutes a 'viable alternative'.

Our members consider a CDR 'measures of success' framework should be developed to support this definition of a viable alternative, which could involve:

a) Adoption rates

Growth in the adoption of CDR by businesses and consumers is the strongest indicator that it presents a viable alternative to screen scraping.

Metrics could include number of active consents, growth in data recipients (including representative and sponsored models), registered software use cases, growth in data holders becoming accredited as recipients and number of businesses switching from scraping to CDR. Qualitative analysis could also be performed to assess the growth of use cases by type and recipient business models over time.[1] Some of this information is readily available on the CDR Provider Register (but not tracked and reported) while other information would need to be collected from data holders, data aggregators and scraping service providers.

We also strongly encourage Treasury to engage in more targeted engagement with two key cohorts – data aggregators and lending businesses reliant on screen scraping:

- Data aggregators and screen scraping providers will be able to provide insights into relative uptake and the volume of users still reliant on screen scraping, including the challenges cited by their clients regarding CDR adoption; and
- Lending businesses and distributors will provide the best insights into the practical constraints which are currently dissuading them from embracing CDR as a 'viable alternative'. Some of these reasons will be unique to the lending space and difficult to quickly resolve – e.g. transaction coding, credit assessment criteria, use of complex distribution channels which require access to data etc.

b) Consent optimisation and ease of connection

Our members have received feedback from users in the CDR consent process that it can be confusing and that the data quality is sometimes sub-optimal. Ultimately, this results in distrust from users and drop-off.

From the user (and authorised business representative) perspective, they need to be able to connect to CDR as easily as they can with screen scraping. Our members propose that clear benchmarks be put in place for significant consent optimisation to take place in CDR before screen scraping is banned. This could include, for example, greater flexibility with consent obligations and an overall streamlining to better align the user experience.

[1] FinTech Australia generates a quarterly report with this information: *Open Banking Ecosystem Map*.

Our members would like to see the ease of connection to CDR to be as convenient as screen scraping. That is, it should be no more challenging for customers to connect to CDR than it is to connect via screen scraping. Specifically, all financial institutions must offer online authentication methods for consents, eliminating the need for outdated and inefficient paper-based processes.

c) Ease of implementation

Implementing and maintaining data accessibility via screen scraping is generally easier and less burdensome than implementing CDR from a technical and resource perspective. This is a major friction point which inhibits uptake of CDR. Our members see this as a significant hurdle for smaller organizations to transition to CDR at present, given the costs involved in doing so and perceptions of relatively low consumer uptake.

While there may be opportunities for smaller players to become CDR enabled through alternative access models (for example, through partnering with an accredited intermediary), there is a perception that the momentum is not yet there.

We have also observed a lack of understanding and awareness about new accreditation/access models and the improvements and enhancements which have already been made to the CDR framework to make it more accessible. Although these have been beneficial for ADRs and opened new use cases, there is little awareness about these new opportunities. For example, the representative model in particular has seen significant growth in popularity over the last year, increasing 79% with 44 new representatives between March and August this year. The Government should do more to promote these successes and change industry perceptions about when CDR will be 'ready'.

d) Completion rate

Our members consider that the completion rate of CDR when compared with screen scraping should be equal or better. There are costs associated with situations where an application (such as a loan) or onboarding is not able to proceed. If a completion does not take place or takes place at a lower rate than it occurs with screen scraping there would be additional costs burdens for the finance industry that may reduce the viability of businesses.

Members report a variety of connectivity differences between screen scraping and CDR – in some cases up to a 20% drop in through-put. Measuring and evaluating the consumer completion rate for CDR is an important metric in determining its viability and what might need to be done to raise consumer willingness to use CDR (e.g. further CX improvements, monitoring for data holders applying dark patterns during authorisation). Alignment with screen scraping completion rates will be a strong motivator CDR uptake.

However, members also note screen scraping has its own reliability issues which can impact completion. As discussed earlier, these issues and disruptions are increasing with data holder use of MFA and bot-detecting technology.

e) Availability of required products and accounts

Our members have indicated that CDR does not currently cover all the products and associated data being accessed and used via statements or screen scraping. One example is SME loan products, members have noted there are a number of gaps in the breadth of SME loan products and the required data fields that have been made available by banks based on their interpretation of the guidance notes / rules. Another similar example members noted is where banks have not enabled CDR for business customers in circumstances where the customer uses the banks' digital banking platform designed for more complex businesses, even though these platforms are used by large numbers of SME businesses that should be in scope for CDR. Some members are concerned that banning screen scraping without addressing these gaps would instead result in a switch back to paper statements for any SME use cases requiring bank data.

e) Data quality/completeness

Our members consider that the quality of data received will need to be of as high quality as that which is received via screen scraping. If the data quality and reliability is insufficient it will be unable to be considered a viable alternative. Many members do not share the view offered in the Discussion Paper that CDR is currently a more stable data-sharing option than screen scraping. However, they also acknowledge these issues can vary depending on the data holder.

As already discussed, we consider it important to assess whether CDR provides the data required by sectors most reliant on screen scraping, like lending, to be able to provide their services without disruption. This could involve a thorough gap analysis through targeted consultation which examines the types and

amount of data that can be collected through screen scraping compared to CDR. It would also serve as an education exercise for businesses with ready made CDR use cases which could significantly boost the ecosystem's active consumer consents.

Members have suggested the ACCC could proactively ensure that data holders have conducted appropriate data quality testing. This could be as simple as providing the test plan along with the results or something more intensive where the testing is done via automation.

Quality issues raised with data holders must also be addressed and rectified promptly.

f) Use restrictions (derived data)

Use restrictions on the handling and use of CDR data can make it less useful than data obtained via screen scraping and unviable for certain use cases. Our members believe there needs to be more flexibility in the use of derived data in line with current use of screen scraped data. For instance, CDR participants should be able to use insights derived from the data themselves without the CDR Rules applying, which is currently only possible when disclosing to non-CDR participants.

Furthermore, our members suggest a clear definition of materially enhanced or derived data whereby CDR Rules no longer apply. This would provide clarity and allow businesses to leverage the full potential of the data they collect, thereby improving their services and offerings to customers.

Ensuring that businesses can use CDR data in a way that is compatible with the primary use cases of CDR, and how businesses are required to use and store data in general, is critical to its viability in the market.

g) Compliance and enforcement

Some of our members believe that there is currently limited incentive for data holders to improve the quality of the data and compliance with CDR requirements. Our members consider more proactive compliance and enforcement from regulators will be critical to driving improvements in data quality and reliability; more in line with what is available through screen scraping.

Our members have identified the need to keep data holders accountable as CDR shifts from a long 'build phase'. Without stronger regulator supervision and

enforcement, data holders are unlikely to invest in improving technologies which will make CDR a less viable alternative. With increased CDR participation, thorough enforcement of the CDR Principals and clear guidelines for different access models will also be important.

What are your views on a ban on screen scraping where the CDR is a viable alternative?

Views on a ban varied greatly between members. However, all at least supported in principle the phasing out of screen scraping, consistent with the 'viable alternative' precondition set out in the Statutory Review of the CDR.

The benefits of CDR over screen scraping are clear. However, as identified throughout our submission there are currently serious gaps in the viability of the CDR as an alternative to screen scraping for all use cases. If these are resolved before a transition to CDR is forced, the market will be significantly more receptive to it and consumers would not be as impacted by the deficiencies in the CDR in return for greater security, transparency and control over their data.

Members are generally supportive of encouraging a graduated transition to CDR in circumstances where CDR is available and a viable alternative. However, some members suggested screen scraping should remain available as a 'back-up' option until issues like CDR data quality, derived data usage restrictions and consent flows are fully resolved.

The Government's ongoing commitment to improving the existing CDR framework will be crucial to it meeting the benchmarks and measures for success outlined earlier in our submission. As acknowledged throughout our submission, many of these initiatives, like improvements to CDR consent and nominated representative processes, are already underway.

Certainty about the future directions of the CDR is another important component. To justify investing in it, prospective CDR recipients need confidence in the framework and its improvement over time. Rather than focusing on perceived delays, emphasis should be given to providing clear timelines and a forward plan for sectoral and functional expansions and operational enhancements.

What timeframe would be required for an industry transition away from screen scraping and why?

Most members consider that any banning process would need to be staged. That is, once a particular performance level is achieved for CDR in a particular sector, only then could screen scraping be banned.

Broadly, the transition process should involve some of the following steps:

- Addressing technical and regulatory challenges based on consultation feedback;
- Further targeted engagement with screen scraping providers and business reliant on it to understand their practical challenges and friction points (including at the product level);
- Educating these stakeholders to encourage a shift away from screen scraping;
- Strengthening compliance and enforcement for data holders;
- Maintaining an ongoing focus on enhancing and improving the CDR framework (e.g. through rules and standards enhancements at a regular cadence);
- Monitoring and measuring the success of CDR adoption and continuing to collect feedback on areas for improvement; and
- Evaluating the effectiveness of CDR adoption and the impact on consumers and end users.

Many members are concerned that banning screen scraping prematurely would be disruptive and result in less competition. There was broad acknowledgement that uplifts and improvements to the CDR framework could drive uptake and obviate the need for a specific ban. Some also raised the importance of screen scraping being available as a back-up.

Other members supported an earlier ban with certainty around timelines in order to drive uptake and switching to CDR and mitigate the risks identified in the discussion paper. They have suggested a ban on new onboarding for screen scraping could be banned as a priority.

Although views vary, members generally consider two years would be required at minimum for an industry transition away from screen scraping where CDR is a viable alternative (i.e. once uplift and improvement milestones have been met/implemented). Consideration would also need to be given to pre-emptive steps taken by banks and other data holders to block screen scraping and whether having certainty about timing would mitigate this behaviour and allow for a smoother transition.