23 October, 2023

Consumer Data Right Policy and Engagement Branch
Market Conduct and Digital Division
The Treasury
Langton Crescent
PARKES ACT 2600

SENT VIA ELECTRONIC MAIL TO: data@treasury.gov.au

Re: Envestnet | Yodlee Response to The Treasury - Screen Scraping – policy and regulatory implications Discussion paper

Yodlee welcomes this opportunity to provide its perspectives in response to the Australian Government The Treasury's ("Treasury") screen scraping – policy and regulatory implications discussion paper. As a data aggregator that has for more than 20 years supported consumers', small businesses', and investors' (collectively "consumers") Intelligent Financial Life™ by providing access to their financial data globally across a vast spectrum of different types of financial accounts, and which has significant experience operating in a highly regulated environment. Yodlee appreciates the opportunity to share its perspectives on some of the questions the Treasury poses in its discussion paper.

About Yodlee

Since inception more than two decades ago, Yodlee has been a leading consumer-permissioned data aggregation platform provider globally. Across the world, our ecosystem empowers more than 37 million customers to access their financial data and utilize products and tools that improve their financial wellbeing. Our consumer-permissioned data aggregation platform has been used to access over 440 million financial accounts and given consumers the opportunity to access a host of different financial products and services in a competitive, consumer-driven ecosystem.

Through the data connectivity that Yodlee provides, consumers regularly access holistic personal financial management tools, account verification solutions, affordable credit, accounting software automation, and better financial advice, among a plethora of other use cases. As a champion of open finance globally, Yodlee believes that consumers are best positioned to determine which financial products, tools, and services may be the most valuable to their unique financial situation.

In Australia, Yodlee has more than 150 clients ("data recipient clients"), servicing more than one million active screen scraping connections to power these use cases. As an Accredited Data Recipient ("ADR"), Yodlee operates as an Outsourced Service Provider ("OSP") for other ADRs, and a Consumer

Data Right ("CDR") Principal for CDR Representative clients. Yodlee is in the early stages of CDR migration, with eight live CDR clients; three ADRs under the OSP model and five CDR Representatives. Yodlee sees significant consumer benefit to APIs versus screen scraping and aspires to move clients to CDR APIs as quickly as possible; however, and as we outline in our responses to specific questions below, in the absence of amendments, certain consumers' data may only be accessed today through screen scraping.

Discussion Paper Responses

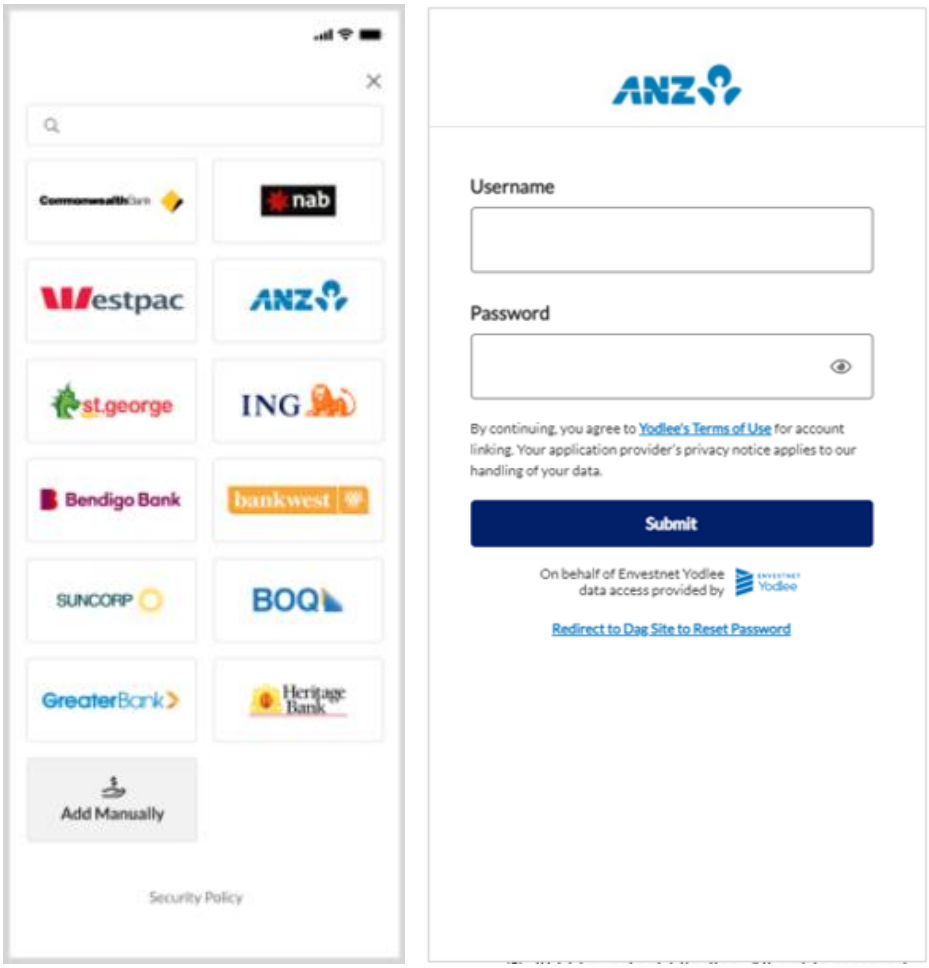
1. What screen scraping practices are you aware of or involved in?

    a. What is the scope and purpose of the data that is captured? Is the data that is captured only banking data, or does it include data from other sectors?

    Yodlee utlizes consumer-permissioned data from the banking sector as well as from other sectors where CDR data is not currently available including wealth, superannuation, insurance, government, multi-currency accounts and non-bank lending. Yodlee captures data for our data recipient clients from large financial institutions and well as FinTechs and small businesses that are less likely to be in scope for CDR in the medium term. Over 50% of our current data recipient clients utilize screen scraped data from data sources beyond the current scope of CDR, primarily wealth investment data. These additional data sources which are not available today through the CDR are essential to the viability of many use cases, especially lending and personal finance management. The impact of banning screen scraping would be quite significant as Yodlee supports over one million active screen scraping connections for Australian consumers.

    b. What steps do consumers, screen scraping service providers and businesses using screen scraping take in the screen scraping process? What information is provided to consumers through the process?

    As an intermediary, Yodlee enables consumers to connect their financial accounts to our clients' applications through our FastLink application. In essence, we provide the connectivity that allows the data to flow from the consumer's financial account to our clients' applications. Before a consumer connects their financial account through Yodlee, they are presented with a consent screen where they are prompted to provide consent for Yodlee to access their financial institutions accounts and their login credentials (i.e., username and password). This screen also includes a link to Yodlee's Terms of Use which explain that credentials may be used to access the data. Yodlee's Terms of Use explain Yodlee's relationship to the consumer, Yodlee's client's relationship to the consumer, Yodlee's use of data, and provide a link to Yodlee's Privacy Access Request Portal for questions related to what data Yodlee holds. In the case of multi-factor authentication, if a one-time passcode is requested by a data provider, Yodlee prompts users for this credential and provides it to the data provider. Once the user provides consent and the user is authenticated, the consumer is redirected back to the clients' application and Yodlee is able to access their financial institution accounts.



c. When is the consumer's data accessed as a one-off, and when is longer-term or ongoing access obtained? Where ongoing access is in place, how are consumers made aware of this and can they cancel access at a later point?

Yodlee follows strict access frequency and data minimization practices. By default, account verification and credit decisioning use cases are configured for one-time access. As a best practice, some account verification data recipient clients call the Yodlee delete API directly following an account verification attempt, to immediately remove the credentials and shared data. Other data recipient clients will retain the connection to enable future balance and transaction refreshes for ongoing servicing of payment or credit use cases.

Personal finance management, wealth management, and small business accounting are common use cases where ongoing access is required. The Yodlee platform utilizes a refresh algorithm based on the consumer's activity. If the consumer is active in the last 30 days, Yodlee will refresh the account once daily on their behalf to power features such as expense and transaction monitoring. As a consumer becomes less active, Yodlee reduces refreshes to between every 3 to 7 days. When a

consumer's last access exceeds 90 days, Yodlee stops refreshing the account until the consumer logs back in and the process is reset.

Ultimately, our client (the data recipient client), owns the relationship with the consumer. The Yodlee platform provides an unregister API that deletes the consumer's data from the Yodlee database when a consumer cancels a service with Yodlee's client. The Yodlee platform also has delete account and delete connection APIs for deleting individual accounts and financial institution connections, including the underlying consumer data.

Yodlee only collects information that is necessary to fulfill the client's use case for the consumer. For example, if a consumer shares their bank and card data for a spending analysis and budgeting application, Yodlee will only obtain accounts and transaction data and not any personal information. For a one-time account verification, Yodlee will only access bank account information and defer from collecting card, loan, or investment information.

All Yodlee platform features for refresh frequency and data minimization are followed for both screen scraped data and CDR data.

d. Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?

No, Yodlee does not use screen scraping for purposes other than consumer-permissioned data collection.

2. Are there any other risks to consumers from sharing their login details through screen scraping?

No response

3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?

Yodlee maintains a comprehensive information security program, policies, and procedures to ensure protection of consumer login details.

4. Could you provide any examples of actions your organisation takes to prevent or block screen scraping (if you hold the consumer's data, such as a bank), or when your company's use of screen scraping has been blocked (if you provide screen scraping services or you partner with a screen scraper to provide your services), and why?

Yodlee has been blocked from screen scraping by several financial institutions in Australia. Yodlee's typical process is to actively work with the financial institution to build trust and awareness of the impact to their customers. Typically, Yodlee performs the following actions:

1) Contact the data provider to articulate the customer impact of blocking access.

2) Negotiate a reversal of data access blocking. Yodlee will review our security posture and data minimization practices with the financial institutions to provide assurance that our processes adequately protect the data.

3) *Partner with financial institutions so they can identify Yodlee screen scraping agents and monitor activity. It is worth noting that Yodlee has had similar challenges in the U.S., where even though Yodlee has a contractual relationship with the financial institutions, they will sometimes block access prior to completing transition to an API. In those instances, Yodlee follows the same procedure as outlined above.*

5. Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?

   Yodlee partners with financial institutions (primarily in the U.S.) that do not have APIs available to actively manage screen scraping thereby providing consumers portability of their data and enabling use of their preferred financial wellness applications. These partnerships give the financial institution transparency into the data Yodlee is accessing and enable them to manage site traffic volumes, limit the data Yodlee is permitted to screen scrape to applicable use cases, and discern between when Yodlee is screen scraping versus a bad actor. Financial institutions provide Yodlee with the appropriate URLs to use for screen scraping access to the data, whitelist Yodlee, and monitor our site interactions.

   In the U.K., where screen scraping has been banned for accessing payment accounts Yodlee works with financial institutions, clients, and consumers to ensure there is a clear delineation between the non-open banking connections (i.e., pension account, mortgage account etc.) that need to be accessed via screen scraping versus the open banking connections that are available via API. Similar to the consent workflow in Australia, Yodlee leverages Yodlee's Terms of Use and the consent screen where Yodlee utilizes user-friendly terminology to delineate between the two types of connections, screen scraping versus API.

6. Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?

   See response to number 7 below.

7. Are there any other international developments that should be considered?

   In the U.S., the Consumer Financial Protection Bureau (CFPB) is in progress of developing a legal framework for open banking and deciding on the future guardrails for the use of screen scraping under its 1033 rulemaking process. The CFPB's proposed 1033 rule is expected to be released by the end of October 2023. In the U.K. and E.U., screen scraping is banned only for accounts covered by PSD2 under the open banking framework. For data not covered under PSD2, screen scraping is still the predominate method of data access. The E.U. and U.K. are both seeking to expand from open banking to open finance so more use cases will be covered by regulation in the near term. In South Africa, screen scraping is the only method for providing consumers access to their financial data, however the Financial Services Conduct Authority is in the process of understanding and implementing an open finance framework for South Africa that would look to use APIs versus screen scraping.

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

   a. Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?

Data is being accessed through screen scraping that is not available via CDR. Sectors where CDR data is not currently available include wealth, superannuation, insurance, government data, multi-currency accounts and non-bank lending. Over 50% of Yodlee's current clients are accessing investment related data through screen scraping. Yodlee captures data for its clients from a variety of data providers including smaller FinTechs and non-bank lenders that may not be in scope for CDR in the medium term. These data providers power use cases for personal finance management, budgeting, and lending.

b. Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?

CDR has a whitelist of allowable scenarios where data can be onward shared with appropriate consent. These scenarios do not always align to the business models of Yodlee clients resulting in continued use of using screen scraping because clients are unable to migrate to CDR. In addition, CDR rules require compliance activities that are above and beyond the Privacy Act increasing the cost of doing business for Yodlee clients which makes clients hesitant to transition from screen scraping to CDR.

For example, until recently CDR Representatives were not permitted to onward share data to outsourced service providers such as firms contracted to perform data enrichment or assist with credit assessments. In addition, use of CDR data with accounting platforms has not been viable until recently due to the broad number of contexts where onward sharing of banking data occurs including through platform API partners but also other ordinary activities such as invoicing and payments. It's easy to identify use cases (e.g., using data derived from CDR data to make a payment) where the current onward sharing rules still make using CDR data difficult.

Under the CDR small business data recipients are subject to additional use restrictions and deletion requirements that do not exist with screen scraping. These regulatory requirements have made it a challenge for small business data recipients to move over to CDR.

Yodlee has also submitted a response to the Operational Enhancements – Consumer Data Right Rules Design Paper. In our response we highlight the potential negative impacts of introducing additional requirements and burdens to the CDR Representative model. In order to ensure CDR is a success, there needs to be a proportionate risk-based approach to any additional requirements placed on firms, especially for those firms looking to utilize the CDR Representative model.

c. Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?

Currently, CDR and the Australia Privacy Act have two distinct sets of privacy requirements with respect to the onward sharing of data. The concept of "CDR data" has created a secondary set of rules that treats this set of personal data as different than other personal data under the Privacy Act. Yodlee recommends aligning CDR privacy protections requirements to existing privacy regulation that covers the requirements for protecting and sharing of all personal information versus separate and distinct requirements for CDR data.

d. Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

The CDR framework needs to be adjusted to be more flexible to support existing use cases and new uses cases as the ecosystem matures. In addition, introducing a risk-based approach to requirements for smaller firms who are seeking to enter the market through the CDR Representative model would be helpful. Incorporating size of the firm, revenue, and volume of consumer accounts into the determination of the level of security and privacy control requirements and providing additional time to meet the full range of requirements would remove some of the barriers to entry.

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

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

    The government should determine if the CDR is a viable alternative based on at least the following four criteria:

        1) *Availability of data providers (e.g., wealth and superannuation are not currently available, so CDR is not viable).*
        2) *Availability of all account types within the sector that are required to enable business use cases.*
        3) *Comparable or better product metrics including measures of consumer friction (i.e., consent flow conversion rates, refresh success rates, availability, etc). These metrics can be use case specific (e.g., business consents currently experience very high friction).*
        4) *Restriction on use of data that prohibit a switch over from screen scraping (i.e. small business example above).*

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

    There still needs to be time for firms (especially smaller firms) to transition to CDR including sufficient time to upgrade technology to be able to consume data from the APIs. In addition, the framework needs to be adjusted for smaller firms to reduce barrier to entry or given time to meet the rigorous CDR requirements. Lastly, the data not only has to be available through CDR but the rules have to have enough flexibility to be able to meet the business requirements of existing use cases.

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

    Yodlee has been operating in the U.S. for over 20 years. Over the last three years, the U.S. has made significant progress in transitioning to APIs through a market led approach but still has a long journey ahead to enable all use cases. Some of Yodlee's US clients still require technology updates to be able to transition from screen scraping to the available APIs.

Yodlee has operated in the U.K. since 2003, when first expanding into the U.K. there was no open banking regulation and Yodlee provided connectivity to consumers bank accounts via screen scraping. In 2018, all that changed when the revised Payment Services Directive came into effect. One of the requirements under PSD2 was that all firms looking to connect to consumers' bank accounts had to be regulated. To become regulated, Yodlee needed to complete and submit an application with the Financial Conduct Authority. That process took over 2 years because Yodlee was required to draft, develop, and meet certain requirements we had not previously been required to meet. Yodlee supports having robust regulation that ensures consumers have portability of their data and that data is protected but we respectfully emphasis the challenge firms can face when trying to meet new requirements. Therefore, we would urge the Treasury and ACCC to provide firms with as much time and flexibility as possible or risk significant impacts to consumers whose only access to some of their data today is through screen scraping.