25 October 2023

Ms Jessica Robinson
Assistant Secretary
Consumer Data Right Policy and Engagement Branch
Market Conduct and Digital Division
Treasury

Via email: data@treasury.gov.au

Dear Ms Robinson

Screen scraping – policy and regulatory implications consultation

COBA thanks Treasury for the opportunity to comment on its discussion paper on the policy and regulatory implications of screen scraping.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has around $160 billion in assets and 5 million customers. Customer owned banking institutions account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market. Our sector's share of ADI housing lending is around 6 per cent and our share of ADI personal lending is around 5 per cent.[1]

COBA member banks have a wide range of business models and service many different demographics including those originating from employee groups (e.g., essential workers) or specific regional areas. The customer owned banking sector has a long history of putting our customers first.

Key points

COBA supports moving away from screen scraping technologies towards the Consumer Data Right (CDR), giving consumers greater control of their own data and harmonising the approach to both privacy expectations and security requirements of safeguarding information, particularly sensitive personal data and banking security codes.

While we support a transition from screen scraping, COBA believes that adequate time needs to be provided to allow our members to transition away from the use of screen scraping to the CDR.

COBA supports move towards Consumer Data Right

In the current environment of increased cyber risk, COBA is supportive of moving away from screen scraping technologies towards the Consumer Data Right (CDR), giving consumers greater control of their own data. Scams and data breaches targeting consumers are becoming increasingly common and sophisticated. They can result in significant financial losses and identity theft which can be highly distressing to consumers.

[1] APRA's Monthly Authorised Deposit-taking Institution Statistics, July 2023: Monthly Authorised Deposit-taking Institution Statistics.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

COBA is aware that some of our member banks use screen scraping third-party providers, for example, to comply with responsible lending obligations under the *National Consumer Credit Protection Act 2009*. We note that the use of screen scraping may be particularly prominent now as many consumers are looking to refinance their home loan to obtain a 'better deal'.

Screen scraping involves consumers disclosing their Internet Banking (IB) login details to third-party providers. This can increase the risk of data available to cyber hackers. While it is common for screen scraping providers to utilise IB credentials once and discard after use, it is possible that in some circumstances, some providers maintain the IB credentials for future use. This creates an additional layer of risk for consumers. A number of banks and third-party providers have moved to blocking or enacting additional authentication consumer friction if screen scraping is detected at IB login.

The sharing of IB login details may also impact consumer behaviour outside of screen scraping, by normalising and legitimising the highly risky behaviour of sharing banking credentials. This practice may lead to consumers being more likely to share credentials or one-time passwords with cyber criminals posing as the consumer's financial institution or screen scraping third party provider. The notion of screen scraping is also contrary to the strong messaging by banks, urging consumers to never share credentials with anyone. COBA expects this strong messaging to continue given the Government and industry focus on anti-scam initiatives and consumer education.

Appropriate transition

While we support a transition from screen scraping, it is COBA's view that adequate time needs to be provided to allow our members to transition away from the use of screen scraping to using CDR as an alternative.

A move from screen scraping will involve considerable changes to systems and processes. Our members need to be given adequate opportunity to prepare for the transition and have submitted a timeframe of between 24 -36 months is appropriate due to the significant operational considerations. These considerations include the following:

- **Time to become an accredited data recipient:** Members would need become an accredited data recipient or CDR representative to receive consumer data. Data holders are also required to meet changing CDR compliance requirements.
- **Operationalising CDR data use:** Sufficient lead time would also be required to operationalise the data aggregation for lending in the CDR environment. The transition from screen scraping to CDR would be a significant activity requiring a project to be established and executed.
- **Examining contractual arrangements:** A transition period would need to enable COBA members to amend existing contractual arrangements as required to disengage from screen scraping activities with providers.
- **Non-bank lenders in the CDR:** Having non-bank lenders participating in CDR would help facilitate a move away from screen scraping, as it would provide a fuller view of the customer's financial situation for the lending data aggregation use case.

We note that it would also be beneficial for any outcomes from the review of the *Privacy Act 1988* regarding proposed changes to CDR Data Standards to be factored into the transition timeframes.

Scope and purpose of data captured by screen scraping

Uses of screen scraping

Some COBA members use third party screen-scraping providers to execute digital data aggregation as part of home loan lending, particularly digital home loan channels. Screen scraping is used to make the home loan application process easier for customers by gathering and verifying their income, expenses

and liabilities digitally. Instead of supplying bank statements, customers will use their IB login details, and the system collects their financial information. The third-party screen scraping provider collects information that is used to assess a customer's credit risk profile. This is in line with ASIC's revised Regulatory Guide 209 Credit licensing: Responsible lending conduct, which refers to digital data capture providing access to information to be utilised as part of a responsible lending assessment process.

In addition to home loan lending, there are also accounting software providers using screen scraping that interacts with business banking accounts. These data feeds from bank accounts are a key feature of the software to help reduce manual data entry and reconciliation.

Steps in the screen scraping process

Steps in the screen scraping process will vary depending on the bank and the third-party screen scraping provider.

In one example provided by a member bank, within a digital home loan application, loan applicants can utilise a service from a third party to assist with data aggregation.

In this example, during the online application process, customers read and consent to the bank's privacy consent and notification form. Customers are also provided with information about the third-party screen scraping provider. Customers are presented with the option in the workflow to speak to a lender offline if they prefer not to connect through the third party. The digital channel is optional, and customers can choose to apply for a loan through a lender.

If the customer is comfortable to connect through the third party, as a step of the application process they will be redirected to a third-party welcome screen, where they are provided with links to the third party's user terms and conditions and privacy policy. The customer must accept these to proceed. The applicant then selects their financial institution from the available list and inputs their IB user and password credentials for that financial institution. The applicant can then select which accounts with that financial institution are to be included in the data sharing. All accounts that the applicant can normally view within IB with that financial institution will be displayed to select from. The applicant can then repeat this process with other financial institutions that the third party can access. For joint applicants, both borrowers will separately complete the third-party process.

Customer access as a 'one off' vs continuous access

COBA is aware of various uses of consumer data including as one off and continuous access.

In one member bank example, consumers' data is accessed as a one-off as part of the third-party digital data aggregation. The customer's financial institution provides the third party with a read-only snapshot of the customer's banking data that is a one-time retrieval only. The customer's IB credentials will not be retained by the third party. After an external security review, the reviewer concluded that the IB credentials are securely deleted from memory (cleared and replaced with zeros).

Managing risks of screen scraping

Member banks or third-party providers may take the following steps to manage privacy and data security risks associated with screen scraping:

- Securely encrypting customers' usernames and passwords with 256-bit encryption, secured by 2048-bit keys. Customers' usernames and passwords are not seen or stored by either party in the transaction.

- Once the account and transaction data has been gathered, the secure connection to a customer's bank is permanently closed. Third party securely discards the credentials after the login attempt has occurred.
- The customer's financial institution provides the third party with a read-only snapshot of the customer's banking data that is a one-time retrieval only. The secure methods for delivering the resultant report payload are Secure File Transfer Protocol (SFTP) or secure URL which support PGP encryption.
- Removal of a customer's IB credentials by the third-party. IB credentials are securely deleted from memory (cleared and replaced with zeros).
- Third party is ISO 27001 and SOC2 compliant, and its software is hosted in Australia without information assets sent or stored overseas.

Comparability of screen scraping and the CDR

One member bank submits that for the digital data aggregation in lending, customers' bank account details and transaction history are accessed to verify the customer's financial information. As part of this, data that originates from non-CDR entities, such as non-bank lenders, is being accessed. It would be useful to have these entities participating in CDR to help facilitate a move away from screen scraping. It is important for our member banks to get a full view of the customer's financial situation for data aggregation.

To successfully execute the digital data aggregation in lending member banks would need become an accredited data recipient or CDR representative to receive consumer data.

Consistent regulatory approach

Screen scraping may potentially remove protections available to consumers under the ePayments Code, leaving the consumer vulnerable to financial loss. Consumers are unlikely to understand this when handing over their credentials to a bank or other credit provider.

Some banks include terms and conditions that do not allow screen scraping technology. For example, in the case of refinance, while a prospective bank may use screen scraping to assess a loan application, the consumer's current bank may ban it in their terms and conditions. Some banks may also detect a screen scraping application and immediately terminate the session. This highlights the difficulties of refinancing or obtaining new credit products when some financial institutions use screen scraping, while others ban them. A move towards a uniform, safer system will benefit both consumers and financial institutions.

If you wish to discuss this submission, please contact Ilana Madjar (imadjar@coba.asn.au).

Yours sincerely

MARK NGUYEN
Chief of Policy