Digital Platform Services Inquiry – Consultation

Equifax Response

7 August 2023

EQUIFAX

Starting in 1967 as the Credit Reference Association of Australia, a mutual and initially for retail stores and later large banks, we remain Australia's leading provider of credit risk and due diligence solutions. Today we employ around 1,000 people in Australia and New Zealand; since 2016 we have been part of Equifax, the global credit reporting group headquartered in Atlanta, USA.

More particularly, in addition to hosting Australia's largest credit reporting body (**CRB**) for consumer credit, Equifax also offers a significant range of consumer identity and fraud mitigation solutions and a commercial credit bureau, as well as risk-mitigation solutions (such as the National Tenancy database), employment verification and, to a lesser extent, marketing services support solutions.

Personal information (**PI**) held as consumer credit reporting information is covered by extensive prescription in Part IIIA of the *Privacy Act 1988* (Cth) (**Privacy Act**), its associated regulations and by additional detail in the Privacy (Credit Reporting) Code 2014 (Version 2.3), authorised by the Office of the Australian Information Commission (**OAIC**). PI held as part of commercial credit information, together with all other PI in Equifax's control, is protected by the Australian Privacy Principles (**APPs**).

ACCC's invitation to Equifax to share views on the data broker industry

The ACCC is calling on consumers, businesses and interested stakeholders to provide submissions about data broker services in Australia, as part of its five-year digital platform services inquiry into markets for the supply of digital platform services in Australia and their impacts on competition and consumers, following a direction from the Treasurer in 2020. Equifax welcomes the opportunity to provide this initial (and any subsequent) contribution to the ACCC's request for information to inform its seventh report on expanding ecosystems of digital platform service providers due to the Treasurer by 30 September 2023.

Equifax provides the details set forth in this paper as an initial response to questions the ACCC has posed to it about its business practices as a data broker in the Australian marketplace and the products and services we create and supply. We also provide our view on whether potential competition and consumer issues may arise in Equifax's supply of data broker services to its customer base ranging broadly from Australian banks and other financial services entities to those businesses seeking data solutions across their business landscape including refinement of human resources processes, management of product and service risk within commercial markets and verification of identity and matters pertaining to tenancy arrangements and financial account conduct.

Equifax aims to be fully transparent in its data broker operations, cognizant of the large amounts of information it provides on Australian consumers and the central role it plays in enabling the exchange of information between businesses in the consumer interest and in the support of

Australian corporates and small businesses and of business integrity, innovation, and growth in the Australian economy.

As a data broker, Equifax develops its own databases of or is provided by third party corporate and business clients, partners, suppliers and other data brokers, information from a very wide range of sources. These data sources include federal and state government agencies like company and business registers, electoral roll, Document Verification Service (**DVS**) and bankruptcy lists, publicly available data, other data brokers, clients and collections agencies.

Types of information collected include names, home and work addresses, age, browsing behaviour, purchasing behaviour, financial status, employment, qualification and tenancy history and a range of other socio-economic and demographic information.

Some of the products and services Equifax creates include audience profiling reports, consumer purchasing data and risk and fraud management products for tenancy, insurance or credit product applications.

In the conduct of its data broker business, Equifax sources data from data brokers and sells products and services to data brokers, as well as non-broker clients.

In response to specific questions asked by the ACCC, this report provides an initial overview of a representative list of products and services Equifax supplies as a data broker, the sources of the data that feeds into those products and services and the customers to whom that data, identified or de-identified or anonymised, aggregated and enriched is provided.

Definitions applied

For the purposes of this report, Equifax applies the definition of 'data broker' as provided in the Ministerial Direction, namely that a 'data broker' is *a supplier who collects personal or other information on persons, and sells this information to, or shares this information with, others*.

In this regard, Equifax applies the definition of 'personal or other information on persons' as '*including information about an identified individual or an individual who is reasonably identifiable, as well as information about an individual that has been de-identified, anonymised, or aggregated*'. This definition is broader than the definition of personal information in the Privacy Act.

As the issues set out in the report and the questions pertaining to these are further developed, our views contained in this document may be subject to further consideration.

EQUIFAX DETAILED RESPONSE TO QUESTIONS POSED BY THE ACCC POSITIONS ON PROPOSALS OF CONCERN AND OF PARTICULAR INTEREST

Market dynamics

Question 1: Who are the data brokers operating in Australia that predominantly collect information from other sources (i.e., not directly from consumers)?

Data brokers in Australia operate within a wide range of industries and organisations.

The three Credit Reporting Bodies (**CRBs**) operated respectively by Equifax, Experian and Illion are data brokers using data sourced from third parties not only to provide credit reporting services to a wide customer base including the financial institutions of Australia but also to provide data driven products for a variety of industries including marketing, data analysis, fraud recognition and prevention and identification verification products. That data may include a combination of demographic (including identity data), geographic, device identification, financial and market research online and offline data.

Australian State and Commonwealth Governments and Australian Courts are also data brokers in that they provide information for a fee to third parties (including Equifax) that then feed that information into their own products and services. The contractual arrangements vary, for example, the Australian Securities and Investments Commission provides its data to Equifax under a data broker agreement.

Other data brokers that predominantly collect information from sources other than directly from consumers include entities such as:

- Fraud and Identity Verification companies such as GB Group, Green ID and Data Zoo who represent that they assist industry by identifying individuals during an online application process;
- News corporations such as NewsCorp Australia that acknowledges in its Privacy Policy that they supplement information collected directly about consumers interacting with them with information from other sources including information from affiliated companies in Australia and internationally;
- Property Information/valuation platforms such as Domain, Real Estate Agency Group of Australia (REA), Infotrack and CoreLogic Australia (a partnership arrangement of certain Australian financial institutions) who operate and market a number of products and services, including property data and analytics services, platform and risk management services;
- Tenancy Data brokers, such as InfoTrack, Dye & Durham, Corelogic and National Tenancy Database (which is powered by Equifax and fully endorsed by REIWA) supplying risk assessment information to thousands of real estate agents;

- Platforms that facilitate individuals' access to their personal credit information, independent of interaction with any credit reporting bureau, for example ClearScore Australia that describes itself as 'a bit like an Amazon of financial services' and Finder;
- Platforms that facilitate commercial reporting access and credit management tools such as CreditorWatch;
- Marketers, loyalty programs and competition sites that collect, collate client lists and identify customer segmentation;
- Consumer Data Recipients that enable access to the Consumer Data Right and provides additional analytical services such as Adatree, Basiq, wych, Finder, Mastercard and Yodlee;
- Online social media platforms such as Meta (Instagram and Facebook) that share information combined with data derived from customer interaction with third parties and partners such as advertisers and audience network publishers, partners who use their analytical services, partners who offer goods or services on the platform owner products and commerce services platforms and integrated partners, measurement vendors and marketing vendors; and
- Data enrichment companies such as Quantium, iD4me, Oracle Australia who provide a 360-degree view of customers across a wide array of data attributes.

Question 2: How do data brokers compete? What factors do data brokers differentiate themselves on (e.g., price, range of data, specific types of data, analysis undertaken, additional services offered)?

Data brokers compete on a range of factors, including:

- Price and pricing structures;
- Range of data and of data sources;
- The ability to offer specific types of data;
- The range and depth of analysis undertaken;
- Range and exclusivity of access;
- Complementarity of data products and services offered;
- Security of data; and
- The depth of experience in the data marketplace, in both Australia and globally.

Equifax competes with other data brokers operating in its fields of business (including but not restricted to the credit reporting bureau business) by differentiating itself on a wide range of factors, including (but not limited to):

- The integrity and capability of its people and processes;
- Experience in operating in highly regulated environments for example, our credit reporting business which has been operating since 1967;
- Its emphasis upon innovation and responsiveness to consumer and market needs;
- Its range of products and services;
- Its transparency and legal compliance;

- The breadth, quality, accuracy and range of value added services, ranging from the supply of data lists for specific purposes, fraud prevention and credential verification services to bespoke data solutions.;
- Its onboarding options, including where appropriate the option to try and test before committing to a product or service;
- Its ongoing servicing and development of strong value driven products and services with strong compliance with regulations and security processes;
- Timely response to consumer and customer complaints; and
- A unified security and privacy controls framework providing for cybersecurity, privacy, fraud prevention, crisis management, and physical security across the Equifax data landscape.

Question 3: How difficult is it for new data brokers to enter the Australian market? What are their entry strategies (e.g., expansion of overseas data brokers into Australia, expansion of other businesses into data broking, new entrants)? Does this differ depending on the types of data products or services provided?

The data broker industry is reasonably easy to enter in Australia as is evidenced by the steady increase in the number of new entrants into the data marketplace. Setting up a data broker business requires:

- The ability to manage a range of data types and data volumes, the quantum of which is determined by the nature of the products and services to be offered;
- Decisions to be made in respect of multi-cloud solutions, social media and Internet of Things;
- Investment in technology, data platforms and conduits;
- Investment in human capital and on-site expertise;
- Investment in legal and compliance expertise and knowledge needed to navigate the complex legal environment; and
- Most importantly, investment in the protection of data privacy and security.

Equifax's acknowledgement of the practical challenges that new entrants into data broking face underpins its new client and product and service onboarding processes. Equifax fosters new entrants into data broking in the sale and provision of its products and services. In fact, many of these actively facilitate new entrants into the marketplace, for example on a reseller or referrer basis.

Equifax nationally and globally welcomes competition in the data marketplace as a major impetus to the development of new data products and services and the fostering of innovative ideas generally in the interests of both businesses and consumers worldwide.

Question 4: What are the benefits of data brokers? Whom do they benefit? Does this vary by data broker? If so, how?

Data brokers enable the exchange of information between businesses and consumers to drive greater informed decision making and ultimately better and safer growth in the Australian economy. The absence of data brokers in the market would significantly restrict access to information in the market to the largest corporations with significant customer sets and the information they have on them.

More specifically, data brokers address many market problems such as the following

- Facilitating the combination of multiple Data Broker services (some offered by Australian Government departments) into a single offering/service, reducing commerce friction, for example DVS, Death Check and Electoral Roll AML/CTF checks;
- Helping consumers to be identified through online ID Verification processes as part of a third party product or service application, while also, in the case of Equifax services, preventing fraudulent activity;
- Improving product offerings and delivering these to consumer segments that may have greater interest and derive more benefit from taking them up;
- Facilitating more cost-effective marketing by small businesses;
- Developing risk mitigation products (for example, identity protection products and verification services) that provide major benefits to both consumers and to the businesses;
- Providing product and service innovation supporting a more flexible and responsive marketplace;
- Facilitating pre-employment credentialing;
- Reducing friction in application processing for products and services;
- Increasing participation rates in new or existing markets for products and services; and
- Supporting and helping grow new data broker entrants through product offerings and existing partnerships.

Question 5: What factors do you consider when choosing which data broker to acquire products or services from?

While Equifax itself is a data broker, it does obtain data products and services from a wide range of other third party suppliers to enhance its own product and service offerings and value propositions. These data brokers from whom we acquire data are subject to a due diligence and screening process. Among the factors Equifax considers for any new data product or service are:

- The source/s of the data collected;
- Customer disclosures that support individual consumer consent;
- The relevance of the data collected;
- The additional benefit the data will add to the product or service;
- The quality and currency of the data collected;
- The integrity of the data during the data life cycle including collection, storage, security and deletion for the life of the arrangement between us;

- The impact of data collected on the security and integrity of the data that we already hold;
- The data broker's security practices in preventing access to PI data provided via Equifax clients using partner services;
- The compliance of all parties, including Equifax itself, with Australian law as to the collection, management, aggregation, use, process of sale and distribution of the data collected;
- The contribution to the strengthening of our enhanced data insights and data;
- The contribution to scaling of new offerings;
- Contribution to our highly differentiated market propositions;
- Possibility to assist our support open data regime to take advantage of this as it evolves;
- Contribution to the development of new market opportunities; and
- Identification of the ability of the data broker to assist us to create products and services to extend our capabilities in new industries and new exchanges.

Data collection and sources

Question 6: What information do data brokers collect? For each type of information, provide details of:

Equifax collects a range of data for use in its product and services such as:

- Personal information of individuals such as name, address, date of birth,
- Certain demographic information,
- Contact information,
- Identification information,
- Biometric information,
- Employment Information,
- Sensitive information such as criminal and medical history (when consented to),
- Property information,
- Company and business information,
- Director information,
- Publicly available information,
- De-identified information, and
- Aggregated information.

a) How this information is collected, including details of any technologies used (e.g., tracking scripts, web-based plug-ins, tracking pixels, or SDKs in apps).

The majority of our services use data provided via Australian Commonwealth and State government enterprises and other data brokers. We also access certain publically available data obtained via the Internet. Where we do collect data from consumers directly, Equifax (or a third party data broker) provides a notification regarding the collection and use.

Equifax collects data directly from third party suppliers either by an API or via web interface third party lodgement.

b) Where or from whom this information is collected.

Equifax has various channels from which we collect or extract data about an individual consumer. Equifax collects information from:

- Australian Commonwealth and State Governments;
- Third party subscribers to Equifax products such as our consumer and commercial credit bureaus and our Fraud bureau;
- Third party aggregators and other data brokers;
- Public internet sites such as data.gov.au;
- Entities located overseas; and
- The individual directly.

In addition to the above, Equifax facilitates the verification of consumer information against various Government data sets where we are accredited as a broker for that purpose.

c) The terms and conditions under which the data is collected.

The terms and conditions under which we collect data include:

- The Equifax Privacy Policy available on our website at www.equifax.com.au/privacy
- The Cookies policy available on our website at www.equifax.com.au/cookies, and
- Privacy and consent notifications within products.

Where data is obtained by third party vendors, Equifax reviews the Terms and Conditions prior to collection of the data and ensures that it is used in line with the purposes disclosed in the Terms and Conditions.

Where data is collected from third parties, the Terms and Conditions have varying levels of customisation based on the negotiation of any particular licensing agreement. Changes may occur to accommodate a vendor request as long as the changes are within Equifax Legal guidelines for risk tolerance in all critical areas including Security, Confidentiality, Compliance, Liability Limitations, Representations and Warranties and Indemnification. Any changes to the business terms must still align with Equifax requirements for data use, security, retention, vendor service levels, termination options, and cost. Similarly, Equifax may require changes to a standard vendor agreement to meet Equifax requirements in the areas cited above. Terms for Data Security are also integral to any data licence agreement Equifax executes.

d) Any prices or fees paid for the information, including details of how these are determined.

Different pricing models apply to different types of data product or service obtained. These include:

- Pricing schema based on a per transaction or per purchase basis;
- Subscription based models; and
- A 'one- off' fee.

Question 7: Are there any particularly important or must-have sources of information for data brokers to collect? If so, what are they and who supplies these (e.g., digital platforms)?

Different products and services require different must-have sources of information. For example:

- Existing Australian Commonwealth and State Governments;
- AML/KYC – related products and services necessarily rely on government and non-government sources of individual identity and transaction information;
- Identity verification data required to support fraud identifications services;
- Property and land titles data;
- General biographic data such as date of birth, marital status, education and employment history, professional affiliations for various ranking purposes such as job candidate checking and ranking and lead scoring;
- Consumer segment market differentiation including through data acquired from government records, websites, social media platforms, Google searches and more; and
- Continued access to public data.

Data brokers are added-value data companies that play a crucial role in the sourcing of data knowledge and data management strategies and process and market analysis that underpins, with the information we independently collect, a plethora of products that enhance both business and consumer data use and experience.

Question 8: What information do you sell or provide to data brokers?

a) To which data brokers? Do you provide or sell the data to multiple data brokers? Why or why not?

Our principal business is to sell data insights to corporate customers. We also sell data in a number of categories to assist a range of data brokers to resell for an identified purpose or commercially refine their products and services and to manage risk.

b) Under what terms and conditions (including price) do you sell this data? Is this done via tender, negotiated contracts, take-it-or-leave-it list prices, or other means?

Equifax data is provided or sold to multiple data brokers with permitted use clauses for each data asset. This is done via:

- Standard contracts that offer products and services on standard terms and velocity pricing,
- Negotiated contracts (the predominant mechanism),
- Licensing arrangements,
- Partnering arrangements,
- Subscription arrangements,
- Reseller and referral arrangements,
- Partnership arrangements, and
- Clear permitted use terms.

The terms and conditions contain provisions that govern restrictions on data use, including maintaining confidentiality and security of the data.

Equifax may accommodate clients' requested changes to its standard licensing agreements subject to such changes comporting with Equifax's risk assessment.

c) How do you collect this data?

Refer to our response to question 6b.

d) Do you know how this data is used? Do you have any control over this?

Equifax contractually imposes specific conditions on the use of data it provides to data purchasers. Prior to contracting, Equifax investigates the context/s in which any data set is to be used.

Question 9: What other types of businesses (non-data brokers) do you sell or provide data to?

Our principal business is to sell data insights to corporate customers to use in respect of the products and services they offer to end consumers and businesses. Equifax offers a range of products and services which use various data sources as detailed in our response to question 11a.

Data products and services

Question 10: What are the business models used by data brokers? How do they monetise their services?

Depending on the nature of the product or service, Equifax monetises its service by a number of pricing models including:

- Price per transaction (for example commercial data products),
- Licensing and subscription fees, and
- Tiered pricing based on the quantum of data used.

Question 11: What types of data products and services are offered by data brokers?

Excluding credit reporting bureau services, Equifax offers multiple products and services as a data broker. This document examines a representative range of our products and services that broadly span the following five categories.

Fraud & Identification Products

Equifax Fraud & Identification products and services include:

- **ID Matrix & DVS** - IDMatrix is the only Australian identity verification service that includes a built-in fraud assessment and compiles the results into a single outcome. Equifax's comprehensive pre-screening can check your customers for known fraud indicators during the verification process. IDMatrix offers a reliable means of matching document data with government records through the Australian Government's DVS, making it easier for organisations to satisfy their identity verification and anti-money laundering and counter-terrorism obligations. The service parameters can be adapted to include an organisation’s own business rules;

- **FraudCheck** - This service provides access to a depth of fraudulent information not available anywhere else in Australia. FraudCheck is a members-only collaborative, knowledge-sharing service designed to stop fraudsters in their tracks. FraudCheck is a fraud detection tool bringing together powerful insights from Equifax's Shared Fraud Database, populated by our Fraud Focus Group (**FFG**). By joining our FFG, a business can use FraudCheck to gain access to an invaluable data source of confirmed fraud events that can be used as an early warning system to identify fraud at the point of application, before substantial losses occur. FraudCheck is one of a kind in Australia, offering a collaborative, knowledge-sharing service of superior fraud intelligence. The pooling of member-provided data assists in the identification of common trends in fraud activity as well as additional intelligence, fraud patterns and market insights. In addition, Equifax

enriches this information by contributing valuable third-party data including police listings; and

- **Biometrics** - clients use biometrics to verify their customer's identity remotely while improving their customer onboarding experience, supporting their compliance requirements and helping to mitigate their fraud risk.

Verification Exchange

Equifax Verification Exchange is a product designed to reduce fraud risk and increase speed of decision making when assessing employment income information, for the purpose of securing finance.

Equifax Verification Exchange uses a data conduit model, as intermediary for an individual consumer (**Applicant**) who is applying for a particular service, where their employment income is required to be verified by the provider of the service (**Verifier**). In using the Equifax Verification Exchange®, the Verifier accesses 'source-of-truth' employment and employment income information with the express consent of that Applicant.

HR-Workforce Solutions

HR-Workforce Solutions products and services include fit2work.

fit2work is Australia's leading provider of background screening checks. We assist over 2400 clients across all verticals including Federal, State and Local Governments, Health Services, Financial Institutions, etc. to keep their organisations safe and compliant. Our portfolio consists of over 45 different types of checks ranging from Identity, Criminal, Financial, Licence and Medical History screening. The checks can be ordered, tracked and reviewed conveniently through our secure online platform or our customers have the ability to integrate their HR System directly with fit2work.

Consumer Portfolio and Insights

Consumer Portfolio and Insights products and services include:

- **Collector Insight.** This product is a premium debt collection tool that provides debt collectors via the IQ Connect platform with information including customer contact details and public data insights to assist with debt recovery.

- **Consumer Audience.** This product integrates demographic, household, neighbourhood, property and event based attributes with financial insights to drive business and marketing success.

Commercial and Property Solutions

Commercial and Property Solutions products and services include:

- **Company Beneficial Ownership Identification**. This product facilitates the determination of beneficial ownership of a non-public company and supports customers in maintaining their Know Your Customer (**KYC**) and Anti-Money Laundering and Counter Terrorism (**AML**) programs as required by AUSTRAC.

- **Land Titles.** Part of Equifax's property solutions, Equifax land title searches can be combined with other relevant property searches, such as property valuations, to make the most informed decisions. We recommend it for a range of businesses including banks and financial institutions, mortgage brokers, collections, insolvency firms, trade credit providers, financial planners, online conveyancing software and government departments.

- **The National Tenancy Database.** This product offers:

    - **Tenant Check**
      This product provides tenant blacklist screening, rental history, bankruptcy information, court judgments and court writs.

    - **Identity Verification** (protecting customers from identity fraud)
      This product validates the identity of tenancy applicants using the market-leading identity verification solution from Equifax.

    - **ASIC & Company Credit Check**
      This product checks the applicant's commercial history using ASIC company data and Equifax commercial credit bureau.

    - **Credit Score on Directors & Commercial Entities**
      This product combines ASIC details with company/director credit file information from Equifax to provide a company risk score.

a) Who acquires these?

Fraud & Identification Products

Customers who acquire Fraud & Identification Products are:

- **ID Matrix & DVS -** Financial services providers including banks and credit card providers.

- **FraudCheck -** Financial services providers including banks and credit card providers.

- **Biometrics** – Financial services providers including those offering products in the sub-prime marketplace and marketing and Accountancy service providers.

- **Global Screening –** Banks and other financial service providers, capital management and investment entities, and global trading businesses.

Verification Exchange

Customers who acquire **Equifax Verification Exchange** are financial services providers including banks and credit card providers.

HR-Workforce Solutions

Customers who acquire the **fit2work** include:

- Health care entities,
- Banks and financial services providers at all tiers,
- Federal and State Government Departments and services,
- Nearly 300 private businesses and organisations,
- Utilities and other service providers, and
- Universities in Australia.

Consumer Portfolio and Insights

Customers who acquire the Consumer Portfolio and Insights products and services include:

- **Collector Insight -** Debt collectors, State Government departments, banks and other financial service providers.

- **Consumer Audience** - Media organisations, digital marketing and collaboration companies and utility providers.

Commercial and Property Data Solutions

Customers who acquire the Commercial Data Solutions products and services include:

- **Company Beneficial Ownership Identification** - Customers include entities such as banks and other financial institutions that wish to determine beneficial ownership of non-public companies as part of their KYC and AML programs.

- **Land Titles** - Customers include banks and other financial institutions,banks and financial institutions, mortgage brokers, collections, insolvency firms, trade credit providers, financial planners, online conveyancing software and government departments.

- **National Tenancy Database** - Customers include real estate agents and those entities that deal with leasing. Individuals can also request copies of their tenancy reports directly from Equifax.

b) How and for what purposes are these used?

Fraud & Identification Products

These products are used by financial institutions, betting agencies and other businesses to assist with identifying fraud, removing fraud risk and satisfying government legislation such as *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 *(Cth*) and the *Anti-Money Laundering and Counter-Terrorism Rules* before funding a loan.

Verification Exchange

This product enables an individual to provide express access consent for their own 'source-of-truth' employment and employment income records to a third party for the purpose of the third party verifying this information is correct in an application.

HR-Workforce Solutions

This product provides background screening checks on prospective employees to keep organisations safe and compliant by offering over 45 different types of checks ranging from Identity, Criminal, Financial, Licence and Medical History screening.

Consumer Portfolio and Insights

These products provide solutions to clients relating to individuals and audiences. Solutions include Portfolio Management and Debt Services (CRB derived data) as well as Marketing Services/Data Driven Marketing. These products use a range of consumer and commercial insights using data segmentation, public data sources to drive insights, obtain new customers, manage customer experience, improve debt collection and reduce costs.

Commercial and Property Solutions

These products and services offer companies with insights to help manage risk, combat fraud, grow profitable customer relationships and comply with government regulations.

c) What terms and conditions (including restrictions) typically apply to their use?

The terms and conditions applying to many of our products and services are broadly available online at https://www.equifax.com.au. The Equifax Australia Information Services and Solutions Pty Limited [ABN 26 000 602 862] Terms of Supply apply and form the agreement for all Equifax and ABR customers in relation to requests for our standard information services and solutions. For details, refer to

https://www.equifax.com.au/sites/default/files/Equifax%20Terms%20of%20Supply%2015062022.pdf

An example of terms and conditions (including restrictions) for a specific product are those applying to:

- Verification Exchange, with terms and conditions available at: https://www.equifax.com.au/hrsolutions/termsandconditions.html under the Equifax Verification Exchange heading, plus the 'Terms of Supply' - all Applicant and Verifier facing terms and conditions are transparent and available on-line.

All parties who provide information to Equifax in respect of its products and services and who obtain and use these products and services must comply with the provisions of relevant Australian legislation, including:

- Privacy Act 1988 (Cth),
- Equifax third party security requirements,
- The Australian Privacy Principles,
- Australian intellectual property law,
- Australian competition law, and
- Modern slavery prohibitions.

Question 12: What products and services have you acquired from data brokers?

a) From which data broker(s)?

Equifax has acquired a number of products and services, data and channels for data delivery from data brokers. Examples include:

- Document Verification Service (Department of Home Affairs),
- Threatmetrix (LexisNexis),
- Australian Death Checks (Coordinating Registry is Queensland Registry of Births, Deaths and Marriages,
- Law courts,
- Australian Securities and Investments Commission,
- Australian Financial Security Authority,
- Australian Communications and Media Authority,
- Market research organisations, and
- Direct marketing companies.

b) Were these bespoke or 'off-the-shelf' products?

Many products, if not the majority in some data areas, are 'off-the-shelf'.

c) Under what terms and conditions (including price) did you acquire these products and services? Was this done via tender, negotiated contracts, take-it-or-leave-it list prices, or other means?

The terms and conditions (**T&Cs**) under which Equifax acquires its products and services are often complex as they cut across a number of data suppliers, both government and private sources. This is well illustrated by the process by which Equifax has obtained the data for the construction of ID Matrix:

- The process of data acquisition T&Cs, including pricing, for the Australian Death Check are set by the Australian Coordinating Authority, the Queensland Registry of Births, Deaths and Marriages (**QRBDM**), in consultation with all State and Territory registries of births, deaths and marriages. Equifax had limited scope for negotiating on T&Cs. We were invited to provide commentary on the proposed commercial model as this was a new initiative developed by the QRBDM. Equifax had to submit an application to become a Data Service Broker. The pricing for this product is tiered.

- The T&Cs, including pricing, for DVS are set by the Dept of Home Affairs in consultation with the relevant Commonwealth, State, and Territory document register owners. Equifax, together with other stakeholders, were invited to comment on the proposed commercial model at the time as this was a new Government initiative to make the DVS available to the private sector. It had previously been restricted to Government agencies. All changes to the T&Cs and pricing have been made by the Department of Home Affairs with very little to no scope for input/negotiation. Equifax had to apply to become a Gateway Service Provider.

- T&Cs for VEVO Business Service (Visa Check) are set by the Dept of Home Affairs. This is a take it as is agreement with no scope for negotiation. There are no fees for access to this service. Equifax had to register for access by applying for an ImmiAccount and have our requested access type verified.

- T&Cs, including pricing, for Email Risk and Device Intelligence, were set by the service provider (LexisNexis), with some scope for commercial negotiations.

d) What did you use these products and services for?

These products and services support the data needs and requirements of Equifax's broad customer base. A product such as ID Matrix facilitates the construction and delivery of a wide range of specific products and services including to government, private and corporate clients.

e) What terms and conditions or restrictions govern or governed the use of these products or services?

There are a plethora of terms and conditions or restrictions that govern the use of these and many of our products and services. These often relate to the security provisions and protection of intellectual property rights, and conditions on the on-selling of the product or service. Use is strictly governed by compliance with relevant law.

Question 13: Are there any 'must-have' data products or services that you acquire from data brokers? Are these available from multiple data brokers? If you were unable to acquire these from a data broker, how else could they be acquired?

There are many 'must-have' data products and services that Equifax acquires from data brokers These include;

- Government sources which provide data not accessible from alternative sources;
- Law courts; and
- Industry bodies such as Australian Communications and Media Authority.

Question 14: How important are data brokers for the provision of digital platform services? For example, in addressing data-related barriers to entry. Why?

Data brokers assist the provision of digital platform services by gathering information from a variety of sources for which it would otherwise be inefficient and/or cost prohibitive for data companies to access on their own account:

- Individuals, and more particularly, from various public web services;
- Publicly available sources, especially those on the internet;
- Third parties (who sell data) to enhance the data sets they hold;
- Third Party companies;
- Community data enabling the identification of top talent, the mitigation of investment risks, market research and HR intelligence;
- Various social media sites that enable their customers to take advantage of data of millions if not billions of individuals the collection of which by their customers would be cost prohibitive;
- Public databases such as court records, criminal records, bankruptcy records, driver's licence, motor vehicle records. Birth certificates, marriage licences, census data, credit card companies and rewards platforms;
- Technographic data to enable targeted marketing, enhance competitive intelligence, monitor the technological landscape;
- Support lead generation, investment and market research; and
- Firmographic data to enable a 360-degree view of companies, the identification of investment opportunities, group companies by filters, track the growth of competitors, support HR and market research.

All of these activities are beneficial to investors, HR tech companies, lead generation companies, and in particular, new entrants into the digital platform provider marketplace. They:

- Support the gaining of competitor knowledge,
- Track and monitor selected companies and consumer market segments,
- Boost deal sourcing,
- Improve and scale lead generation, and
- Enable platform service providers to enrich their existing data and refine their services.

Question 15: How do the products and services provided by data brokers affect competition in other markets? For example, in markets where businesses may supply data to data brokers, or in markets where businesses acquire products and services from data brokers in order to provide their own products and services. If the products and services provided by data brokers do affect competition in other markets, how?

Equifax believes that the products and services it provides as a data broker places those entities who use them in a stronger position to compete in their markets. The ways in which they do this include:

- The provision of more granular knowledge of businesses' consumer customer base with the ability to market their products and services in a more targeted way to the benefit of the business and its consumers;
- The provision of knowledge of the marketplace that allows for the more effective management of legal and commercial risk;
- The provision of means by which businesses can verify important customer information that allows them to check and report suspicious activity such as fraudulent use of identity, qualification records and employment records that allows the business to compete more efficiently in their marketplace;
- The maintenance on receipt of data of that data's sovereignty and security;
- The support of AML and KYC programs by sourcing PEP and Sanctions data directly from government registries around the world, including the US supplied OFAC List and the Australia supplied DFAT List and RBA List, along with many more from other countries and enhanced lists provided by Accuity; and
- The ability to be able to perform an electronic identity verification of an individual and assess the fraud risk associated with the individual's information provided.

Potential consumer and small business harms

Question 16: What benefits do data broker products and services provide to consumers and small businesses?

The products and services Equifax provides as a data broker to consumers and small businesses help to:

- Prevent fraud, by offering a risk mitigation product preventing fraudsters form impersonating unsuspecting consumers,
- Improve product and service offerings,
- Deliver the most relevant advertisements to consumers,
- Enrich data businesses by allowing for the leverage of individual, census, social media and company data for lawful business purposes,
- Reducing friction in application processing systems,
- Increasing overall inclusion in the provision of products and services, and
- Benefits of a single streamlined government data process.

Equifax data products and services provide inestimable value to consumers and small businesses. An example is the Verification Exchange that is designed to help lenders lower their loan application processing time and associated costs with potential for flow-on of cost benefits to consumers, while also providing a mechanism to assist them to comply with legislative obligations.

Question 17: What consumer harms may arise from the collection, processing, analysis or storage of information by data brokers? Which consumers are most likely to be harmed and why?

An obligation of the data brokerage process is to enrich, cleanse, and analyse consumer profiles before licensing or selling them to third parties to use. Consumer harm can arise where individual profiles are inaccurate or incomplete. This may harm the consumer by leading to:

- Inaccurate or inappropriate profiling;
- Exclusion of the consumer from accessing or obtaining the product they need;
- Breach of privacy, and
- Data breaches.

An effective corrections and complaints process is needed to ensure data that is obtained, held and used is accurate and up to date.

Consumer harm can also arise from inadequate security controls across the data collection, storage, aggregation, de-identification and supply process. A failure to keep data secure can bring cyber risk to broad consumer groups. For this reason, cyber security is a priority at Equifax. There always exists, however, the possibility of potential harm to consumers in the event of a data breach which results in bad actors getting hold of consumer personal information.

Consumer harm can also arise when consumer data is collected, used or provided to other parties without the consumer's knowledge in circumstances where notification is required or outside the parameters of the consumer consent. The risk of this harm is higher when a data broker buys, repackages or sells the data of individuals with whom they have no direct relation. The due diligence processes applied by Equifax to its data vendors and purchasers seeks to safeguard against this possibility.

Question 18: What consumer harms may arise from the use of data products and services sold or provided by data brokers? Which consumers are most likely to be harmed and why?

As a data broker, Equifax is very conscious of and mitigates against:

- Error in risk mitigation products that may deprive consumers of the benefit of a product in the marketplace;
- Scoring processes in some of the marketing products may not be visible to consumers nor easily understandable by them; and
- Storing data for the authorised time exposes that data to security risk. It is for this reason that Equifax places highest priority on safeguarding the security of the data it holds.

At the same time, Equifax acknowledges that due to the billions of data records held by data brokers and the complex multi-layered nature of the business, it may be that some consumer data has been collected and on-sold without the relevant consumers' knowledge in circumstances where notification is required or full awareness of the consent that they have given for it to be provided to third parties. Some consumers may not be aware that data brokers combine and analyse data obtained from both offline and online sources.

Question 19: What processes and controls do data brokers have in place to protect consumers? This may include efforts around the de-identification and aggregation of data, data verification processes to ensure data is accurate, or measures to protect stored data.

Processes and controls data brokers put in place to protect consumers include:

- Notification and informed consent obtained from individuals where required for data that is being collected, used or onsold;
- Contractual requirements including definition of permitted use, compliance with law and data security controls;
- Review to ensure appropriate use within the notification or consent provided;
- Measures to ensure data quality and data maintenance;
- Consumer access and correction rights;
- Measures to remove bias;
- Measures to explain customer or segment scores;
- De-identification where appropriate; and
- Controls on storage of data to ensure deletion once past legal storage requirements.

Of particular importance to the protection of consumers is the application of strict security requirements and protocols including:

- Limited return of PI data when an enquiry is made to protect the data;
- Encryption of data at rest;
- Data classification for data handling and storage purposes;
- Control of access permissions; and

- Product risk assessments.

The particular challenge is that there is not a universal source of truth that is permitted to be used to verify accuracy. This is why data brokers look to acquire data from multiple sources that is permitted for this purpose and can be cross referenced. It is important to be able to use multiple linked data sources to verify an individual and to maintain recency.

a) Are these controls adequate? What more could/should be done?

Equifax applies strong data security, access and use controls across its product and service lines and systems. We are constantly reviewing and updating these to ensure that they remain adequate. Any need for remediation or remodelling of data handling or of the management of data systems generally is promptly attended to. Our move out of physical data centres into the cloud has increased our management and security of access controls and provided for increased encryption of Equifax data.

Question 20: To what extent are consumers aware that their data is being collected and used by data brokers? How are they made aware?

Consumers are made aware of the collection and use of their data by Equifax via:

- The Privacy Policy available on the Equifax website;
- Product and service specific consent, for example the ID Matrix solution advises consumers as to the collection of the data and obtains their consent for the data to be used for identity verification purposes. The consent can be collected directly for individuals that use the IDMatrix white-label website, or it can be collected indirectly by the organisations that use IDMatrix; and
- Consumer data obtained from third parties has been collected with appropriate notification and consent, where required.

Question 21: What steps can consumers currently take to inspect and/or remove the data that is held about them or to otherwise raise a complaint with data brokers?

Equifax provides consumers with rights of access, corrections and complaints in respect of its products and services, with details set out in its privacy policies on the Equifax Australia website.

Question 22: What bodies or resources exist to assist and support consumers in their dealings with data brokers? What more could be done to better educate and empower consumers?

The Australian data marketplace (like any global data marketplace) is extraordinarily complex for consumers to navigate. Even though there is a range of bodies to assist and support them, including with information on their dealings with data brokers, the sheer number and variety of data collectors and brokers and the multivarious websites through which they operate make it

very difficult for many consumers to identify to whom they should speak and how they should navigate the complaints and enquiry process.

Australia regulates data privacy and data protection through a mix of federal, state and territory laws each of which provide for a consumer complaints process. These vary, however, as regards the obligation of participating entities to provide proactive consumer education designed to make consumers aware of the full extent of processes that apply to the collection, use and sharing of their data:

- The Privacy Act and the Australian Privacy Principles (**APPs**) contained in the Privacy Act apply to private sector companies (including body corporates, partnerships, trusts and unincorporated associations) with an annual turnover of at least $3million AUD, and all Commonwealth Government and Australian Capital Territory Government Agencies.

  The Privacy Commissioner has authority to enforce the Privacy Act and the protections it provides to individual consumers and to seek civil penalties for serious breaches or repeated breaches of the APPs including where the entity in breach has failed to put in place appropriate remedial actions.

- Most States and Territories in Australia (except South Australia and Western Australia) have their own data protection legislation applicable to relevant state and territory government agencies and private businesses that interact with state and territory government agencies. The following Acts provide obligations relating to complaints handling processes:

  - *Information Privacy Act 2014* (ACT),
  - *Information Act 2002* (NT),
  - *Privacy and Personal information Protection Act 1988* (NSW),
  - *Information Privacy Act 2009* (Qld),
  - *Personal Information Protection Act 2004* (Tas), and
  - *Privacy and Data Protection Act 2014* (Vic).

- Additionally, there are other parts of State, Territory and Commonwealth legislation that relate to data protection. For example, the following all impact privacy and data protection for specific types of data and activities:

  - *Telecommunications Act 1997* (Cth),
  - *Criminal Code Act 1993* (Cth),
  - *National Health Act 1953* (Cth),
  - *Health Records and Information Privacy Act* 2002 (NSW),
  - *Health Records Act 2001* (Vic), and
  - *Workplace Surveillance Act 2005* (NSW).

- The Commonwealth Consumer Data Right (**CDR**) allows the consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. The CDR provides a mechanism for access to a broader range of information within designated sectors than is provided by APP 12 of the Privacy Act, given that it applies not only to data about individual consumers but also to business consumers and related products. This assists the consumer - but only if they are aware of the relevance of the CDR to them and have the literacy and language levels that facilitate their navigation of its processes of consumer data protection that it provides.

  As it is implemented, the CDR regime will broadly address competition, consumer, privacy and confidentiality issues, and it is a significant support to consumer data rights that it is regulated by the ACCC and the OAIC.

Specific regulators have also expressed an expectation that regulated entities should have specified data protection processes in place. For example, the Australian Prudential and Regulatory Authority (**APRA**) requires financial institutions to comply with Prudential Standards, including APRA Prudential Standard CPS 234 Information Security (CPS 234) and ASIC regulates corporations more generally.

It is clear that more needs to be done to both educate and empower consumers as key participants in the data ecosystem that the legislation informs. In respect of this, the new Privacy laws likely to be put in place by the end of this year or in 2024 - arising from the Attorney General's 'Privacy Act Review Report' (published in February 2023) - may further support the consumer in their interaction with data brokers. If a number of the 116 proposals for reform are adopted, the Australian privacy landscape, including data brokers' operations within it, will be reshaped. It is possible that the realisation of some of the following key proposals will add positive initiatives in the consumer interest if they are accompanied by a community wide education program on data knowledge and security:

- The requirement to act fairly and reasonably when collecting, using and disclosing personal information (Proposal 12) judged on an objective standard and regardless of consent;
- A broader definition of 'personal information' to 'information or an opinion that relates to an identified individual'), allowing the definition to capture a broader range of information (Proposals 4.1-4.4). Such a change would bring the language of the Privacy Act definition in line with the language used in the GDPR definition of 'personal data'; ;
- Direct right of action to enforce privacy rights (Proposal 2) for individuals who have suffered loss or damage as a result of an interference with their privacy. This would allow individuals and representative groups to seek compensation in the Federal Court of the Federal Circuit and Family Court of Australia;
- The requirement to conduct Privacy Impact Assessments (Proposal 13) for any 'high risk privacy activity' which would encompass activities 'likely to have a significant impact on the privacy of individuals';

- Introduction of the concept of processors and controllers in Australian law, making it more aligned with the GDPR (Proposal 22); and
- More specific regulation of targeted advertising (Proposal 20) through a prohibition on the use of information related to an individual (including personal information, de-identified information, and unidentified information (such as internet tracking history) for targeted advertising and content to children, and prohibitions on using sensitive information for targeted advertising and content for any individuals.

It is important to be aware in considering the protection of consumer information that the Privacy Act and the APPs do not regulate the personal information contained in employee records such as training, membership of professional associations, tax, banking and superannuation details and personal and emergency contact details (this is known as 'the employees records exemption'). Australian privacy law also does not recognise categories of 'data processors' or 'data controllers' nor the concept of data processing.

The *Data Availability and Transparency Act 2022* (Cth) established a new best practice scheme for sharing Australian Government Data that ensures that all data is lawfully collected, created or held by a Commonwealth body or on its behalf. Data can include personal and business data. The scheme is underpinned by the safeguards and processes set out in the DATA scheme. The National Data Commissioner also delivers education and support for best practice data handling and sharing, handles accreditation of users, complaints and assessments and investigations and takes enforcement actions.