Print whole section

Australian Financial Crimes Exchange (AFCX) data–matching program protocol

Information on our AFCX data-matching program for the period of 2024–25 to 2026–27.

Last updated 11 August 2025

AFCX data-matching program overview

Objectives and purpose of our AFCX data-matching program.

AFCX data

Data we collect under our AFCX data-matching program.

Notifying the public of the data-matching program

How we notify the public about our AFCX data-matching program.

Variation to the guidelines

Matters considered for variation to the guidelines.

Our lawful role

Our legislative functions and the policies and procedures we follow for a data-matching program.

Why we undertake data matching

Why we conduct data-matching programs and the costs and benefits of data matching.

How we undertake data matching

Systems and processes we use in data-matching activities.

Data quality

How we assure data is fit for use and quality assurance processes we undertake.

QC 105359

AFCX data-matching program overview

Objectives and purpose of our AFCX data-matching program.

Last updated 11 August 2025

Program overview

The Australian Financial Crimes Exchange (AFCX) data-matching program, conducted by the Australian Taxation Office (ATO), outlines our use of AFCX data for 2024–25 to 2026–27 financial years.

One of our key focus areas is strengthening system integrity and controls by preventing, detecting, and responding to evasion and fraud in the tax, superannuation, and registry systems. To further enhance our ability to identify and contain fraud in near real time, we are adopting industry best practices and implementing new fraud prevention capabilities. The ATO became an AFCX member in May 2024 to exchange data and intelligence that anticipate new financial crime behaviours and typologies, as well as identify fraud and tax crime attempts.

AFCX is an independent organisation formed by major banks that operates consistent with not-for-profit principles to assist businesses combat financial-related crimes. The AFCX is a key initiative of the Scam-Safe Accord that requires all member banks to join the AFCX to disrupt, detect, and respond to scams. Banks and financial institutions play an important role in helping reduce the ease with which criminals can 'cash out' a fraudulent refund.

AFCX intelligence will be used to enhance protection of taxpayers' information against identity crime-enabled fraud attacks on our systems by informing the implementation of additional controls on taxpayer records. AFCX data will increase our ability to identify, prevent, detect and monitor suspicious bank account details, IP addresses, and other indicators of identity crime and fraudulent activities, in support of benefits to the Australian community.

Program objectives

Our data-matching programs help us fulfil our responsibility to protect public revenue and maintain community confidence in the integrity of the tax and superannuation systems.

The objectives of our AFCX data-matching program are to:

- protect taxpayer records from identity crime and unauthorised access by detecting, preventing and mitigating risks of unlawful registration, lodgment, and refund fraud
- build intelligence about scam, fraud and crime activities and threats in the financial ecosystem to strengthen integrity of the tax and superannuation systems and develop treatment strategies
- address new and emerging risks through enhanced intelligence capabilities to reduce the impact of financial scams and crimes on

taxpayers, mitigate tax revenue risk and protect the Australian community

detect, investigate and prosecute perpetrators of financial crime activity including identity takeover, money laundering or serious and organised crime.

Why we look at AFCX data

Our AFCX data-matching program will allow us to identify and address a number of tax and superannuation risks, including:

- identity crime
- fraudulent registration
- lodgment of false and fictious tax forms
- refund fraud
- tax fraud enablers.

For more information see:

- The ATO joins the Australian Financial Crimes Exchange | Treasury Ministers
- Our focus | Australian Taxation Office
- Tax crime explained | Australian Taxation Office
- What is tax fraud? | Australian Taxation Office
- Refund fraud | Australian Taxation Office

QC 105359

AFCX data

Data we collect under our AFCX data-matching program.

Last updated 8 August 2025

How we use AFCX data

The data collected under this program will be used to:

- protect taxpayer accounts from identity crime and unauthorised access by implementing safeguarding controls to enable pre-lodgment detection and treatments to victims of fraud, as a preventative measure
- identify, detect, monitor and treat new emerging risks and behaviour patterns which may significantly impact the integrity of the tax and superannuation systems
- compare to our records and other data holdings, as part of the methodologies, including risk modelling outcomes, by which we select taxpayers for compliance activities
- provide insights through models and analysis that support our regulatory approach, to reduce the impact of financial scam and crime.

Previous related programs

Evidence from a pilot program indicated that the AFCX data can improve and strengthen our controls to detect, disrupt and deter tax fraud more efficiently and effectively in near-real time.

The continued collection of AFCX data will be used to enhance our fraud detection capabilities to protect taxpayer accounts.

The data helps us to:

- increase knowledge and understanding of scam, fraud and financial crime threats pose to the tax and superannuation systems
- measure the effectiveness of fraud treatment programs
- bring consequences to perpetrators of fraud.

Data providers

We are the matching agency and, in most cases, the sole user of the data obtained during this data-matching program.

Data will be obtained from the AFCX. The AFCX is a key initiative of the Scam-Safe Accord that requires all member banks of the Australian Banking Association and Customer Owned Banking Association to join the AFCX. This is to strengthen the wider financial ecosystem to disrupt, detect, and respond to scams and financial crimes.

Eligibility as a data provider

We adopt a principles-based approach to ensure that our selection of data providers is fair and transparent.

- The AFCX coordinates the sharing of data and intelligence across the public and private sector to combat scams and financial crime.
- The AFCX operates a business in Australia that is governed by Australian law.
- The data owner provides data-sharing services for the years in focus.
- There are no alternative legislated providers on the market.

The data provider for this program will be reviewed annually against the eligibility principles.

AFCX data disclosure

The disclosure of this data is in accordance with a Participant Services Agreement between AFCX and ATO.

Privacy Act

Data will only be used within the limits prescribed by Australian Privacy Principle 6 (APP6) contained in Schedule 1 of the Privacy Act and in particular:

- APP6.2(b) – the use of the information is required or authorised by an Australian law
- APP6.2(e) – the ATO reasonably believes that the use of the information is reasonably necessary for our enforcement-related activities.

Data elements we collect

We collect various datasets from AFCX including bank account details and IP addresses used in fraudulent activities identified and reported by AFCX members.

The data is obtained from AFCX in accordance with the Participant Services Agreement between AFCX and ATO. The collected data may contain all, or a selection of, the following fields.

Client identification details – individuals

Client identification data elements for individuals that we collect may include:

- given and surname(s)
- date(s) of birth
- addresses (residential, postal, other)
- Australian business number (if applicable)
- email address
- contact phone numbers
- identity verification document details
- employment details
- IP addresses.

Client identification details – non-individuals

Client identification data elements for non-individuals that we collect may include:

- business name
- addresses (business, postal, registered, other)
- Australian business number
- email address
- contact phone numbers
- IP addresses.

Bank account transaction data elements

Bank account transaction data elements we collect may include:

- bank account details
- transaction date
- transaction time
- amount
- IP address.

Number of records

We expect to collect approximately 500k records annually. AFCX data contains entity level identifiable and personal information in non-mandatory fields. Approximately 70k individuals are expected to be affected by this data collection each financial year.

Data retention

We collect data under this program for all financial years from 2024–25 financial year to 2026–27 financial year. AFCX data is collected weekly in the 2024–25 financial year and is made available for use in the ATO's enterprise data environment. Daily ingestion of the data is expected to be in place from the 2025–26 financial year.

We retain each financial year's data for 5 years from receipt of the final instalment of verified data files from the data provider.

The data is required for this period for the protection of public revenue as:

- a retention period of 5 years enables us to cross-reference taxpayer records retrospectively who might be subject to identity takeover or victims of scam or fraud
- the data enhances our ability to identify taxpayers who may not be complying with their tax and super obligations or promoting unlawful behaviour, which is integral to protecting the integrity of the tax and superannuation systems
- retaining data for 5 years supports our general compliance approach of reviewing an assessment within the standard period of review and aligns with the requirements for taxpayers to keep their records

- the data is also used in multiple risk models, including models that establish retrospective profiles over multiple years aligned with period of review
- the 5-year retention period enables us to perform extended analyses of trends and changes in financial crime behaviours and typologies
- destruction of the data would inhibit our ability to identify taxpayers who may be subject to administrative action and therefore result in loss of public revenue.

While increased data retention periods may increase the risk to privacy, we have a range of safeguards to manage and minimise this. Our systems and controls are designed to ensure the privacy and security of the data we manage.

QC 105359

Notifying the public of the data-matching program

How we notify the public about our AFCX data-matching program.

Last updated 11 August 2025

How we notify the public

We notify the public of our intention to collect AFCX data for 2024–25 financial year to 2026–27 financial year by:

- publishing a notice in the Federal Register of Legislation gazette in the week starting 11 August 2025
- publishing this data-matching program protocol on our website at **Data-matching protocols**

- advising AFCX that AFCX - Privacy Policy - AFCX should include that personal information is disclosed to ATO for data-matching purposes.

Gazette notice

The following information about the data-matching program appears as a gazette notice in the Federal Register of Legislation.

Gazette notice: Commissioner of Taxation - Notice of an AFCX data-matching program 11 August 2025

The Australian Taxation Office (ATO) will acquire relevant account and transaction data from Australian Financial Crimes Exchange (AFCX) for the 2024–25 financial year through to 2026–27 financial year.

The data items include:

- client identification details (names, addresses, phone numbers, dates of birth, identity verification document details, IP addresses etc)
- bank account transaction details (bank account details, transaction date and amount, IP addresses etc).

We estimate that records relating to approximately 70,000 individuals will be obtained each financial year.

For this data-matching program, we will match AFCX data against ATO records and other data holdings.

The data collected under this program will be used to:

- safeguard taxpayer accounts from identity crime by implementing protective controls to enable pre-lodgment detection and application of treatments to victims of fraud
- identify, detect, monitor and treat new emerging risks and behaviour patterns which may significantly impact the integrity of the tax and superannuation systems
- compare to our records and other data holdings, as part of the methodologies by which we select taxpayers for compliance activities

- provide insights through models and analysis that support our regulatory approach, to reduce the impact of financial scam and crime.

The objectives of this program are to:

- protect taxpayer records from identity crime and unauthorised access by detecting, preventing and/or mitigating risks of unlawful registration, lodgment, and refund fraud
- build intelligence about scam, fraud and crime activities and threats in the financial ecosystem to strengthen integrity of the tax and superannuation systems and develop treatment strategies
- address new and emerging risks through enhanced intelligence capabilities to reduce the impact of financial scams and crimes on taxpayers, mitigate tax revenue risk and protect the Australian community
- detect, investigate and/or prosecute perpetrators of financial crime activity including identity takeover, money laundering or serious and organised crime.

A document describing this program is available at **ato.gov.au/dmprotocols**.

This program follows the Office of the Australian Information Commissioner's (OAIC) (2014) *Guidelines on data matching in Australian Government administration* (the guidelines). The guidelines include standards for the use of data matching as an administrative tool in a way that:

- complies with the Australian Privacy Principles (APPs) and the *Privacy Act 1988* (Privacy Act)
- is consistent with good privacy practice.

A full copy of the ATO's privacy policy can be accessed at **ato.gov.au/privacy**

Variation to the guidelines

Matters considered for variation to the guidelines.

Last updated 8 August 2025

Submission to the Information Commissioner

The following is the submission we made to the Information Commissioner.

The Australian Taxation Office (ATO) is seeking approval for our Australian Financial Crimes Exchange (AFCX) data matching program 2024–25 to 2026–27 to vary from one or more of the conditions detailed in Guidelines 3.4(a)iv, 6 and 10 of the Office of the Australian Information Commissioner's (OAIC) (2014) *Guidelines on data matching in Australian government administration* (the guidelines).

We are seeking that you exercise your discretion and allow us to simplify the description of the information exchanged and, in limited circumstances, to take administrative action in response to a match without immediately notifying the individual concerned.

A taxpayer may be unaware that their identity has been taken over to access their tax account to update bank account and contact records and lodge a tax form to claim a fraudulent refund. When an unauthorised access or fraudulent activity is detected, the ATO may apply treatments to protect the taxpayer information and account prior to contacting the taxpayer to verify their identity. We also may need to cancel or amend a lodged tax form with the correct data that we hold, to ensure the taxpayer's reporting position is correct and they are protected from negative consequences that may include unexpected debts to third parties and loss of access to Government payments.

This deviation of the normal notification conditions in this circumstance is in the public interest as these adjustments:

- proactively safeguard taxpayer personal information from unauthorised access and identity crime
- protect the tax, superannuation, and registry systems by containing fraud and tax crime attempts in near real time

- fulfil our responsibility to protect public revenue and maintain community confidence in the integrity of the tax and superannuation systems
- ensure that we can prevent ATO fraud while not giving criminals or threat actors detail on specific ways to circumvent the detection measures in place within the AFCX and its member organisations.

We recognise that simplifying the descriptions of the data collected may appear to impact on transparency. However, this impact must be balanced against the need to mitigate effects on the AFCX in responding to and preventing financial crime affecting its members, their customers and the Australian public. This program will be subject to an evaluation within 3 years which is consistent with the requirements of Guideline 9.

Additional information justifying this variation is included in the following tables:

- Table 1 – matters considered in accordance with Guideline 10.2 in seeking this variation
- Table 2 – consistency with requirements of the other guidelines issued by the Office of the Australian Information Commissioner

Matters considered in accordance with Guideline 10.2

This section outlines matters considered against the requirements of Guideline 10.2 in seeking this variation.

Table 1: matters considered in accordance with Guideline 10.2

Guideline	Matter considered	Consideration
10.2.a	The effect that not abiding by the guidelines would have on individual privacy	We have in place very secure processes for handling and storing data. Once acquired, all data will be stored on our secure computer systems where access is strictly controlled, and

		full audit logs maintained. The ATO and our staff operate under stringent confidentiality and privacy legislation that prohibits the improper access to or disclosure of protected information. These obligations are supported by significant penalties, including imprisonment. This substantially mitigates the risks of breaches of privacy.
10.2.b	The seriousness of the administrative or enforcement action that may flow from a match obtained through the data matching program	The administrative action assists the taxpayer to protect their personal information from being stolen, misused or compromised. Where we propose to take administrative action where a taxpayer may have reported incorrectly, we will differentiate between those that try to do the right thing and those that set out to deliberately avoid their obligations. Documented procedures, including the Taxpayers' Charter and compliance model will be followed to ensure fairness and consistency.
10.2.c	The effect that not abiding by the guidelines would have on the fairness of the data matching	There will be no effect on the fairness of the program or the ability of taxpayers to find out the basis of decisions that

	program — including its effect on the ability of individuals to determine the basis of decisions that affect them, and their ability to dispute those decisions	impact them or their ability to dispute those decisions. In limited circumstances, when we detect unauthorised activities, we will apply treatments to protect the taxpayer information and account from identity takeover crime prior to contacting the taxpayer to verify their identity. If we need to amend a tax form, taxpayers are notified of the adjustment in their notice of assessment. This approach is to avoid unfair and unreasonable delays for processing a tax return and delaying a refund. Other discrepancies require verification. Before any administrative action is undertaken, taxpayers will be given a reasonable period to verify the accuracy of the information that has been derived from this data matching program. Where administrative action is to be undertaken, we will adhere to the principles established in the Taxpayers' Charter and compliance model to ensure an equitable and consistent approach is taken. If a taxpayer doesn't agree with an assessment, they maintain the right to dispute the decision.

		They also have the legal right to appeal against those decisions through the courts and tribunals.
10.2.d	The effect that not abiding by the guidelines would have on the transparency and accountability of agency and government operations	There will be no adverse effects on the transparency and accountability of government operations. Publishing our data matching program provides education and awareness of how we use data. ATO data matching is conducted to address identified risks more efficiently. A comprehensive description of the data provider is included in the program protocol. The description also identifies the principles and criteria for selecting the data provider. Our practice is to raise awareness of the data we hold and why it is necessary for our operation. The program protocol is submitted to the Office of the Australian Information Commissioner, and we will strictly adhere to the commitments in that document. We will publish a notice with general information about the program in the Federal Register of Legislation - Gazettes before administrative action starts. We will also make a copy of the

		program protocol available on our website.
10.2.e	The effect that not abiding by the guidelines would have on compliance of the proposed data matching program with the Australian Privacy Principles in the Privacy Act 1988 and the Australian Government Privacy Code	The data is collected solely for the stated objectives established in the data matching program protocol.
10.2.f	The effect that complying with the guidelines would have on the effectiveness of the proposed data matching program	The effectiveness of the program would be reduced if we were not able to use AFCX data to support intended ATO actions to prevent, detect and respond to fraud. Notifying the public of specific types of identity documentation collected by the AFCX provides criminals and threat actors with information that they can use to develop more sophisticated ways of perpetrating fraud and avoid detection.
10.2.g	Whether complying fully with the guidelines could jeopardise or endanger the life or physical safety of information providers or could compromise the source of information provided in confidence	Not abiding by all the requirements of the guidelines would not influence or affect the personal safety of any individual identified as part of the program or compromise the source of the information provided in confidence. There is a risk that publishing the data

		descriptions provided in their entirety would compromise the operations of the AFCX member organisations by alerting threat actors to ways to circumvent existing controls.
10.2.h	The effect that complying fully with the guidelines would have on public revenue – including tax revenue, personal benefit payments, debts to the Commonwealth and fraud against the Commonwealth	Not allowing the exemption under the current program may result in the Commonwealth foregoing taxation revenue and losing community confidence in the integrity of the tax and superannuation systems. Abiding by all of the requirements of the guidelines will reduce the effectiveness of the proposed activity. We would miss the opportunity to prevent unauthorised activities, protect taxpayer personal information and contain fraud and tax crime attempts in near real time. The effect of abiding by all of the requirements in the guidelines could negatively impact both public revenue and the confidence the public and government have in the ATO as an administrator of the taxation system. By sharing information, analytic capability, and evidence-based insights, AFCX members work outside traditional silos to identify criminal

		trends, activity and networks that operate across different businesses. Complying fully with the guidelines may compromise the broader benefit the AFCX provides in breaking down silos to protect the Australian public from fraud,scams and taxation fraud.
10.2.i	Whether complying fully with the guidelines would involve the release of a document that would be an exempt document under the *Freedom of Information Act 1982*	Upon receipt of a freedom of information request, only information relating to the taxpayer's own affairs and to which they are entitled under the Act will be released to the taxpayer concerned.
10.2.j	Any legal authority for, or any legal obligation that requires, the conduct of the proposed data matching program in a way that is inconsistent with the guidelines.	The AFCX has legal obligations to its member organisations to protect the data collected from their customers. Publishing the types of documents used to verify an individual's identity would provide criminals and threat actors with information that could be used to circumvent existing controls. As a member the ATO also has an obligation to abide by the restrictions agreed to by the AFCX and other members. The Commissioner of Taxation, or his authorised representative, has formed the opinion that this data is required to enable us to effectively

		and efficiently carry out its legislated functions under the general powers of administration contained in: Section 3A of the *Taxation Administration Act 1953* Section 8 of the *Income Tax Assessment Act 1936* Section 1-7 of the *Income Tax Assessment Act 1997* Section 356-5 in Schedule 1 of the *Taxation Administration Act 1953* The reasons for proposing to operate outside requirements of the guidelines are detailed above.

Consistency with requirements of the guidelines

This section outlines where we are being consistent with the requirements of the guidelines.

Table 2: consistency with requirements of the guidelines

Guideline	Purpose	Action taken/to be taken
Paragraph 6	Status of the guidelines	Our commitment to complying with the guidelines is embedded in our data management policies and principles and clearly stated in the chief executive instruction.

Guideline 1	Application of the guide	We apply the guidelines for all data matching programs where it is anticipated the program will include records of 5,000 or more individuals. We recognise that programs where there are multiple data sources but with common objectives and algorithms are treated as a single data matching program.
Guideline 2	Deciding to carry out or participate in a data matching program	We conduct a cost-benefit analysis and consider alternate methods prior to proposing to conduct a data matching program. Further, we have rigorous governance arrangements, processes and system controls in place to protect the privacy of individuals.
Guideline 3	Prepare a program protocol	Prior to conducting a data matching program, we prepare a data matching program protocol, submit this to the Office of the Australian Information Commissioner and make a copy publicly available on the ATO website. When elements of a data matching program change, the protocol is amended, a copy of the amended protocol is provided to the Office of the Australian Information Commissioner and updated on our website.
Guideline 4	Prepare a technical standards report	Documentation is prepared and maintained so as to satisfy the requirements of

		a technical standards report.
Guideline 5	Notify the public	We publish notification of our intention to undertake a data matching program in the Federal Register of Legislation - Gazettes prior to the commencement of the program. This notice will include the following information as required by the guidelines: • a brief description of the objectives of the data matching program • the matching agency and (where appropriate) source entities involved in the data matching program • a simplified description of the data contained in the data set involved in the data matching program • the categories of individuals about whom personal information is to be matched • the approximate number of individuals affected • reference to our privacy policy. Notification of the program is also published on our website and data providers are advised they can advertise their participation in the data matching program.
Guideline 6	Notify individuals of proposed	In limited circumstances, a notification occurs after the administrative action. When

	administrative action	we detect unauthorised activities, we will apply treatments to protect the taxpayer information and account from identity takeover crime prior to contacting the taxpayer to verify their identity. Where we take administrative action to amend a taxpayer's tax form based on the data we hold, we are seeking to notify individuals in the notice of assessment. When considering administrative action, we take a differentiated approach between those that try to do the right thing and those that set out to deliberately avoid their obligations. Documented procedures, including the Taxpayers' Charter and compliance model, will be followed to maintain taxpayer rights and obligations. When we identify a discrepancy that requires verification, taxpayers will be contacted by phone, data matching letter or email. Taxpayers will be given a reasonable period to verify the accuracy of the information that has been derived from this data-matching program before administrative action is undertaken. If a taxpayer doesn't agree with an assessment, they maintain the right to dispute the decision. They also have the legal right to appeal against those decisions through the courts and tribunals.

Guideline 7	Destroy information that is no longer required	We regularly review our requirement to continue to retain data and destroy those datasets no longer reasonably necessary.
Guideline 8	Don't create new registers, data sets or databases	We don't create new registers or databases using data obtained in the course of a data matching program.
Guideline 9	Regularly evaluate data matching programs	Programs are evaluated within 3 years of the start of the data matching program. These evaluations are provided to the Office of the Australian Information Commissioner on request.
Guideline 10	Seeking exemptions from Guideline requirements	When we intend to vary from the requirements of the guidelines, we seek the approval of the Office of the Australian Information Commissioner and provide documentation to support the variance.
Guideline 11	Data matching with entities other than agencies	We undertake our own data matching programs. This function is not outsourced. Where data is obtained from an entity other than an individual, we usually do so using our formal information gathering powers. In these instances the entities are advised they are able to notify their clients of their participation in the data matching program.
Guideline 12	Data matching with exempt agencies	We don't usually undertake data matching with agencies that are exempt from the operations of the *Privacy Act 1988* under section 7 of that Act and

		that are subject to the operation of the guidelines that is, any data matching undertaken with an exempt agency would usually be for fewer than 5,000 individuals). In the event a data matching activity would otherwise be subject to these guidelines except for the exemption status, we still adhere to the principles of the guidelines and prepare a program protocol, seeking to vary from the guidelines by not publicly notifying of the program and publishing the protocol. We would still lodge a copy of the protocol with the Office of the Australian Information Commissioner.
Guideline 13	Enable review by the Office of the Australian Information Commissioner	We would not prevent the Office of the Australian Information Commissioner from reviewing our data matching activities and processes. These activities and processes have been reviewed by the Australian National Audit Office and Inspector-General of Taxation.

QC 105359

Our lawful role

Our legislative functions and the policies and procedures we follow for a data-matching program.

Last updated 11 August 2025

Our powers of administration

The ATO is the Australian Government's principal revenue collection agency. The Commissioner of Taxation has responsibility for ensuring taxpayers meet their tax and super obligations.

We follow the Office of the Australian Information Commissioner's (OAIC) (2014) *Guidelines on data matching in Australian Government administration* (the guidelines) in our data-matching activities.

Our data-matching programs help to ensure that Australians are fulfilling their tax and super obligations.

This information forms part of all data-matching program protocols.

We take our obligations seriously. Failure to address non-compliant behaviour has the potential to undermine community confidence in the integrity of the tax and superannuation systems and our capability to administer those systems.

We carry out our legislated functions through general powers of administration contained in but not limited to:

- section 3A of the **Taxation Administration Act 1953**
- section 8 of the **Income Tax Assessment Act 1936**
- section 1-7 of the **Income Tax Assessment Act 1997**
- section 43 of the **Superannuation Guarantee (Administration) Act 1992**
- section 356-5 in Schedule 1 of the *Taxation Administration Act 1953*.

Data matching is one of the strategies used to provide assurance that taxpayers are meeting their obligations. It helps us to identify and deal with non-compliant behaviour.

Data-matching guidelines we follow

Our data-matching programs follow the Office of the Australian Information Commissioner's (OAIC) (2014) Guidelines on data matching in Australian Government administration (the guidelines).

These guidelines help us and other government agencies use data matching as an administrative tool in a way that:

- complies with the Australian Privacy Principles (APPs)
- complies with the Privacy Act 1988 (Privacy Act)
- is consistent with good privacy practice.

The Privacy Act

The Privacy Act 1988 (Privacy Act) regulates how personal information is handled by certain entities, such as companies and government agencies.

Schedule 1 of the Privacy Act lists the 13 Australian Privacy Principles (APPs). The principles cover the collection, use, disclosure, storage and management of personal information.

Data will only be used within the limits prescribed by the APPs and the Privacy Act.

The Australian Government Agencies Privacy Code, embeds privacy in all government agency processes and procedures. It ensures that privacy compliance is a priority in the design of our systems, practices and culture.

We comply with the code's requirements, and we are transparent and open about what information we collect, hold and disclose. We train our staff to keep personal information safe, and all our systems and offices are protected and secure.

Our data stewardship model upholds our data governance practices and embeds 6 ethical standards that guide how we collect, manage, share and use your data:

1. Act in the public interest, be mindful of the individual.
2. Uphold privacy, security and legality.
3. Explain clearly and be transparent.
4. Engage in purposeful data activities.

5. Exercise human supervision.
6. Maintain data stewardship.

Find out more about how we protect **your privacy**.

How we protect your personal information

Our staff are subject to the strict confidentiality and disclosure provisions contained in Division 355 of Schedule 1 to the *Taxation Administration Act 1953*. Penalties include terms of imprisonment in cases of serious contravention of these provisions.

Keeping data safe

Data-matching programs are conducted on our secure systems that comply with the requirements of the:

- Australian Government Information Security Manual produced by the Australian Cyber Security Centre, which governs the security of government information and communication technology (ICT) systems
- Australian Government Protective Security Policy Framework, which provides guidance on security governance, personnel security, physical security and information security.

All ATO computer systems are strictly controlled according to Australian Government security standards for government ICT systems, with features including:

- system access controls and security groupings
- login identification codes and password protection
- full audit trails of data files and system accesses.

For more information see **Online security**.

Data destruction

All information and records are managed in accordance with the provisions of the Archives Act 1983.

The requirement to retain data is reviewed on an ongoing basis in accordance with the timeframes and requirements of the OAIC guidelines. We destroy data that is no longer required, in accordance with the *Archives Act 1983* and the records authorities issued by the National Archives of Australia, both general and ATO-specific.

Under section 24 of the Act, records can be disposed of where it is approved by the National Archives; required by another law, or a normal administrative practice that the Archives approves of.

Approval from National Archives is normally provided through records authorities, which are used in the process of sentencing to make decisions about keeping, destroying or transferring particular information and records.

General or ATO-specific records authorities issued by National Archives apply to our processes of verifying and assuring taxpayer compliance with tax, super and other laws administered by the ATO.

Our record management practices allow us to satisfy the OAIC guidelines and Australian Privacy Principle 11 (APP 11) contained in Schedule 1 of the *Privacy Act 1988* and in particular:

- APP11.1 – An APP entity must take reasonable steps to protect information from
  - misuse, interference and loss
  - unauthorised access, modification or disclosure
- APP11.2 – APP entity must take reasonable steps to destroy or de-identify information it no longer needs.

Our on-disclosure provisions

In very limited and specific circumstances, we may be permitted by law to disclose individual records to other government agencies.

Division 355 of Schedule 1 to the *Taxation Administration Act 1953* sets out the government agencies we can disclose taxpayer information to, and the circumstances in which we are permitted to make those disclosures.

These include agencies responsible for:

- state and territory revenue laws

- payments of social welfare and health and safety programs for determining eligibility for certain types of benefits and rebates
- overseeing super funds, corporations and financial market operators to ensure compliance with prudential regulations
- determining entitlement to rehabilitation and compensation payments
- law enforcement activities to assist with specific types of investigations
- domestic and international partners under tax disclosure and tax treaty arrangements
- policy analysis, costing and effectiveness measurement.

Each request for information by other agencies will be assessed on its merits and must be for an admissible purpose allowed for by tax laws. In specific permissible circumstances, on-disclosures may include de-identified datasets for statistical analysis.

QC 105359

Why we undertake data matching

Why we conduct data-matching programs and the costs and benefits of data matching.

Last updated 11 August 2025

Meeting our accountability

To effectively administer the tax and superannuation systems, we are required in accordance with the law to collect and analyse information concerning the financial affairs of taxpayers and other participants in the Australian economy.

In addition to our administrator responsibilities, the Public Service Act 1999 (PS Act) requires each agency head to ensure their agency complies with legislative and whole-of-government requirements.

Agency heads are required to ensure proper use and management of public resources as per the Public Governance, Performance and Accountability Act 2013 (PGPA Act).

We consider and undertake a range of alternatives to data matching to ensure entities are complying with their tax and super obligations. Relying only on data that we already hold is of limited value for the following reasons:

- The tax system operates on willing participation, so our data is derived from taxpayers that are correctly registered and meeting their lodgment obligations.
- The only other way of ensuring that taxpayers are reporting their obligations correctly would be to contact every taxpayer directly.

Uses of data matching

Data matching allows us to cross-reference suitable external data to identify taxpayers who may not be in full compliance with their obligations, as well as those that may be operating outside the tax and superannuation systems. It also reduces the likelihood of unnecessarily contacting taxpayers who are complying with their tax obligations.

Data matching is an effective method of examining the records of thousands of taxpayers. We do this to ensure compliance with lodgment and reporting obligations. This would otherwise be a resource-intensive exercise.

Data matching also assists us to effectively promote voluntary compliance by notifying the public of risk areas and activities under scrutiny.

Costs and benefits analysis

The costs of our data-matching activities are more than offset by the benefits.

Costs

There are some incidental costs to us in the conduct of data-matching programs, but these are more than offset by the total revenue protected. These costs include:

- data analyst resources to identify potential instances of non-compliance
- compliance resources to manage casework and educational activities
- governance resources to ensure compliance with the guidelines and Privacy Act
- quality assurance processes to ensure the rigour of the work undertaken by analysts and compliance staff
- storage of the data.

Benefits

The use of data is increasingly common across government agencies and the private sector. Data, data usage, computer power and storage continue to grow, which increases the benefits from data matching.

Data matching and the insights it provides help us:

- deliver tailored products and services, which underpins our culture of service
- make it easier for taxpayers and agents by providing tailored messages in our online services
- enable early intervention activities, as our goal is prevention rather than correction
- maintain community confidence in our ability to administer the tax and superannuation systems, because we can
  - make better, faster and holistically smarter decisions with measurable results to deliver a level playing field for all
  - solve problems and shape what we do for the community
  - advise government and deliver outcomes with agility
- maintain the integrity of the tax and superannuation systems by
  - providing education to assist taxpayers to do the right thing
  - deterring behaviours so taxpayers adhere to their obligations
  - detecting taxpayers who are not complying with their obligations, targeting those that continue to deliberately abuse the tax and

superannuation systems

- enabling enforcement activity and recovery of tax revenue
- directing compliance activities to assure that wider risks to revenue don't exist.

QC 105359

How we undertake data matching

Systems and processes we use in data-matching activities.

Last updated 8 August 2025

Data-matching process

When required, our data-matching process uses both mainframe-based and mid-range applications that comply with an ATO-designed software solution (technical standard). The technical standard supports all our data-matching programs and aligns with OAIC guideline 4.7.

We use over 60 sophisticated identity-matching techniques to ensure we identify the correct taxpayer when we obtain data from third parties. These techniques use multiple identifiers to obtain an identity match. The identity-matching process appends matching information to the original reported transaction to include an ATO identifier number and a 3-character outcome code that indicates to the user the level of matching confidence for the transaction. For example, where a name, address and date of birth are available, all items are used in the identity-matching process. Very high confidence matches will occur where all fields are matched.

Additional manual processes may be undertaken where high confidence identity matches do not occur, or a decision taken to destroy data no longer required. Our manual identity-matching process involves an ATO officer reviewing and comparing third-party data identity elements against ATO information on a one-on-one basis,

seeking enough common indicators to allow confirmation (or not) of an individual's identity. We commonly call this process manual uplifting.

Data analysts use various models and techniques to detect potential discrepancies, such as under-reported income or over-reported deductions. Higher risk discrepancy matches will be loaded to our case management system and allocated to compliance staff for actioning. Lower risk discrepancy matches will be further analysed, and a decision made to take some form of compliance or educational activity, or to destroy the data.

To maintain integrity of the administration of the tax and superannuation systems, only staff with a direct and genuine ‘need to know’ can access the technical standards for our identity and discrepancy-matching solutions.

Where administrative action is proposed, additional checks will take place to ensure the correct taxpayer has been identified. The taxpayers will be provided with the opportunity to verify the accuracy of the information before any administrative action is taken.

How we amend a return

We may use data to provide tailored messages for individual taxpayers in our online services. This will prompt taxpayers to check they are correctly meeting their reporting obligations.

In limited circumstances where we identify inadvertent mistakes, we may amend a tax return with the correct data that is available to us.

If you disagree with the decision we made about your information, you can **request a review by lodging an objection**.

After a return is lodged, where we identify a discrepancy that requires verification, we will contact the taxpayer usually by phone, letter or email. Taxpayers will have a reasonable period to verify the accuracy of the information and respond before we take administrative action.

For example, where discrepancy matching identifies that a taxpayer may not be reporting all their income, but it appears they're reporting the income in another taxpayer's return, they will be given the opportunity to clarify the situation.

The data may also be used to ensure taxpayers are complying with their other tax and super obligations, including registration

requirements, lodgment obligations and payment responsibilities.

In cases where taxpayers fail to comply with these obligations, after being reminded of them, we may instigate prosecution action in appropriate circumstances.

Where a taxpayer has correctly met their obligations, the use of the data will reduce the likelihood of contact from us.

In limited circumstances we may use data from a data-matching program to correct mistakes without notifying individuals in advance. When we do so, we will seek an exemption from the Australian Information Commissioner.

Making a privacy complaint

Our **privacy policy** outlines how we collect, hold and disclose data and explains what you can do if you're not satisfied with the way your information has been treated.

If you're not satisfied with how we have collected, held, used or disclosed your personal information, you can **make a formal complaint**.

If you're not satisfied with the outcome of the privacy complaint, you can contact the Office of the Australian Information Commissioner.

For more information, see how we protect **your privacy**.

QC 105359

Data quality

How we assure data is fit for use and quality assurance processes we undertake.

Last updated 11 August 2025

Quality assurance processes

Quality assurance is integrated into our processes and computer systems and applied throughout the data-matching cycle.

These assurance processes include:

- registering the intention to undertake a data-matching program on an internal register
- risk assessment and approval from the data steward and relevant senior executive service (SES) officers prior to any data-matching program being undertaken
- conducting program pilots or obtaining sample data to ensure the data-matching program will achieve its objectives prior to full datasets being obtained
- notifying the OAIC of our intention to undertake the data-matching program and seek permission to vary from the data-matching guidelines (where applicable)
- restricting access to the data to approved users and access management logs record details of who has accessed the data
- quality assurance processes embedded into compliance activities, including
  - review of risk assessments, taxpayer profiles and case plans by senior officers prior to client contact
  - ongoing reviews of cases by subject matter technical experts at key points during the life cycle of a case
  - regular independent panel reviews of samples of case work to ensure our case work is accurate and consistent.

These processes ensure data is collected and used in accordance with our data-management policies and principles and complies with the OAIC's Guidelines on data matching in Australian Government administration.

How we ensure data quality

Data quality is a measure to determine how fit-for-purpose data is for its intended use. It is valuable because it helps us to understand the data asset and what it can be used for.

Data quality management allows us to use data with greater confidence and assists in meeting data governance requirements and ensures a greater understanding of the data we hold.

The ATO Enterprise Data Quality (DQ) framework provides clarity and structure to our management of data quality and may be applied in determining how business areas can make effective and sound use of data.

This framework outlines 6 core DQ dimensions:

1. Accuracy – the degree to which the data correctly represents the actual value.
2. Completeness – if all expected data in a data set is present.
3. Consistency – whether data values in a data set are consistent with values elsewhere within the data set or in another data set.
4. Validity – data values are presented in the correct format and fall within a predefined set of values.
5. Uniqueness – if duplicated files or records are in the data set.
6. Timeliness – how quickly the data is available for use from the time of collection.

To assure specific data is fit for consumption and the intended use throughout our data-matching programs, the following data quality elements may also be applied:

- Currency – how recent the time period is that the data set covers.
- Precision – the level of detail of a data element.
- Privacy – access control and usage monitoring.
- Reasonableness – reasonable data is within the bounds of common sense or specific operational context.
- Referential integrity – when all intended references within a data set or with other data sets, are valid.

Data is sourced from providers' systems and may not be available in a format that can be readily processed by our own systems. We apply additional levels of scrutiny and analytics to verify the quality of these datasets.

This includes but is not limited to:

- meeting with data providers to understand their data holdings, including their data use, data currency, formats, compatibility and natural systems

- sampling data to ensure it is fit for purpose before fully engaging providers on task
- verification practices at receipt of data to check against confirming documentation; we then use algorithms and other analytical methods to refine the data
- transforming data into a standardised format and validating to ensure that it contains the required data elements prior to loading to our computer systems; our data quality practices may also be applied during this transformation process
- undertaking program evaluations to measure effectiveness before determining whether to continue to collect future years of the data or to discontinue the program.

QC 105359

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice

endorses you or any of your services or products).