Program Protocol

Data Matching
between
Medicare and Centrelink records
and
Information about Sumo customers affected by February 2024 data breach

Table of Contents

1. Program Protocol

1.1 Purpose

The purpose of this program protocol is to:

- provide an overview of the program
- outline the objectives of the data matching of Medicare and Centrelink records held by Services Australia with information about the Sumo customers affected by a data breach in February 2024 (**Data Breach**)
- detail the entities involved and the data to be provided by Sumo as the source entity
- outline the technical controls proposed to ensure data quality, integrity and security in the conduct of the program
- describe the matching process, the output produced and the entities that will use the results of the data match
- outline the possible action taken in relation to the results of the program
- specify any time limits on the conduct of the program
- indicate what form of notice is to be given, or is intended to be given, to individuals whose privacy is affected by the program.

1.2 Requirement for a Program Protocol

The Office of the Australian Information Commissioner's (**OAIC**) *Guidelines on data matching in Australian Government administration* (**Data Matching Guidelines**) specify that a program protocol be prepared by agencies conducting certain data matching programs. The guidelines assist Australian Government agencies to use data-matching as an administrative tool in a way that complies with the Australian Privacy Principles (**APPs**) and the *Privacy Act 1988* (**Privacy Act**) and are consistent with good privacy practice. These guidelines are voluntary, but they represent the Information Commissioner's view of best practice. Services Australia complies with these guidelines.

Services Australia's Privacy Policy outlines how a person may lodge a complaint about how their personal information has been handled by the agency and outlines how the agency will deal with such a complaint. Services Australia's Privacy Policy is available at servicesaustralia.gov.au/privacy

1.3 Definition of data matching

Data matching is the comparison of two or more sets of data to identify similarities or discrepancies. In the context of this protocol, the term data matching means the use of computer techniques to compare data found in two or more computer files to identify customer records at increased risk of identity compromise. Once confident matches are found, additional security precautions will be applied. Investigation may be required to protect customers from identity compromise and prevent fraud against the Commonwealth.

2. Data matching program

2.1 Overview of the data matching program

Services Australia administers a range of programs to deliver payments and services on behalf of the Commonwealth. Services Australia maintains the integrity of these payments and services by undertaking activities to ensure customers meet qualification and payability rules, and where required, recover any incorrectly paid benefits. Services Australia also maintains the integrity of the information held, and disclosed to, the agency, to ensure the privacy of our customers.

This program aims to identify records of Centrelink and Medicare (Services Australia) customers at risk of identity compromise as a result of the Data Breach:

- If the Medicare number or Centrelink Reference Number (**CRN**) for an individual was disclosed as part of the Data Breach, Sumo will provide Services Australia with identity information (including Medicare number or CRN) for each affected individual.
- Services Australia will match this data against existing Medicare and Centrelink records to identify customers with compromised identity information that could be used for fraud against the compromised identity or Services Australia.

Identity crime can result in significant financial loss to individuals, organisations, and the Commonwealth. Fraudsters try to use compromised identities to falsely claim Services Australia payments and services in the names of other innocent individuals, who are not otherwise entitled, and unaware of benefits being paid. Identity crime can take the form of theft, as well as manipulation and fabrication, which may result in the creation of new identities, which can grow and remain a burden on agencies and organisations, including Services Australia.

Services Australia will assist affected Centrelink and Medicare customers in a number of ways to prevent and respond to identity fraud (see section 6 of this program protocol). However, Services Australia customers who have been notified by Sumo that their information has been compromised as a result of the Data Breach, should have heightened awareness of suspicious or unexpected activity across all of their online accounts.

2.2 Objectives

The key objectives of this program will assist Services Australia to:

- identify Services Australia customers who have been affected or potentially affected by the Data Breach
- provide additional protection for customers at risk of identity compromise
- undertake targeted detection for suspicious activity on suspected compromised identities to ensure payments and services are provided to the right individual
- take action to address any fraudulent activity, which may result in suspension/cancellation of payments. Suspension or cancellation activities would only occur where a customer account has been hijacked and action is required to protect the customer's identity and/or government outlays.

The data matching will enable Services Australia to take appropriate action to prevent further harm to Services Australia customers affected or potentially affected; provide support to customers; and disrupt fraud. This will allow Services Australia to respond rapidly to protect customers whose identities are compromised.

These objectives are consistent with the social security law principles of administration[1] including:

- the establishment of procedures to ensure that abuses of the social security system are minimised
- the delivery of services under the law in a fair, courteous, prompt and cost-efficient manner
- the development of a process of monitoring and evaluating delivery of programs with an emphasis on the impact of programs on social security recipients.

[1] *Social Security (Administration) Act 1999,* section 8

2.3 Data match scope

The scope of this program is restricted to data matching:

- Medicare and Centrelink records held by Services Australia
- Identity information about Sumo customers where their Medicare number or CRN was disclosed as part of the Data Breach.

3. Agencies involved

3.1 Source entities

This program covers the collection and matching of personal information obtained from Sumo with data in Medicare and Centrelink records held by Services Australia.

Where a customer's Medicare number or CRN was disclosed as part of the Data Breach, the following data, where captured by the Data Breach and available to Sumo, will be voluntarily provided by Sumo to Services Australia:

- card number, expiry date and customer name appearing on Medicare or Centrelink concession card
- customer's date of birth
- customer's home address and telephone number.

Where a Medicare or Centrelink card has expired, the data may contain personal information of individuals who are not currently customers of Services Australia payments or services.

3.2 Matching agency

Services Australia is the matching agency involved in this program and is responsible for:

- receiving the data from Sumo
- matching the Sumo data with Medicare and Centrelink customer records
- the destruction of non-customer data at the end of each matching process.

3.3 Primary User Agency

Services Australia is the user of the results of the data matching. It will receive the data from Sumo and will match it to Services Australia's own data. The results of the data matching will only be used by Services Australia for the purpose of section 9 of this protocol.

4. Data Issues

4.1 Data Quality

Poor quality data is of limited value in data matching. Services Australia will verify the quality and integrity of the data received from Sumo before seeking to match it.

The agency applies systems driven business rules to identify where data does not meet a high standard of data quality, e.g. to confirm that all dates of birth contain a day, month and year, that mobile phone numbers contain 10 digits, and that CRNs are a valid number.

Services Australia will not use data that does not pass data quality assurance processes in the administration of activities described in this program.

4.2 Data Integrity

The agency maintains a high level of data integrity and takes measures to maintain these integrity levels, including designing systems that will not accept records that are incomplete and identifying and correcting records that have data items that are inadequate or corrupt.

Measures taken to maintain integrity levels include:

- designing systems that will not accept incomplete records
- identifying records for matching that have data items that meet data integrity standards.

4.3 Data Security

Services Australia has negotiated the transfer of data from Sumo using a secure email facility, secure document sharing platforms approved for government use (such as SIGBOX) or Physical transfer (IronKey USB).

Where required, prior to transfer of the data to Services Australia's network, the data is cleansed by specialised staff, using a stand-alone off-line device.

Where data has been cleansed and is safe to migrate onto the Services Australia's network, it is then stored in a secure shared drive controlled by the relevant Services Australia team. The shared drive is hosted within Services Australia's data centres in Australia.

The shared drive is managed by specialist staff and access is controlled through role-based approvals. Only staff with a business need will be able to view the data provided under this program.

Access to Services Australia's data centres is strictly controlled and entry properly authorised. Services Australia's security system provides protection and control of dataset access, system entry and program integrity. Security features include logon identification codes, passwords, 2 factor authentication and security groupings to ensure that access to information is on a needs only basis.

Services Australia staff are also subject to statutory secrecy and confidentiality provisions, including under the:

- Social Security (Administration) Act 1999
- Human Services (Medicare) Act 1973
- Health Insurance Act 1973
- National Health Act 1953
- Public Service Act 1999
- Criminal Code Act 1995.

Services Australia is also an agency subject to the *Privacy Act 1988*.

5. The Matching Process

5.1 Identity Matching

Identity matching involves using key data fields provided in external data and comparing these with customer data held by Services Australia. The result of this is establishment of a high-confidence link between external data and customer records held by Services Australia.

Services Australia will carry out the matching of data provided by Sumo with Medicare and Centrelink customer records.

Steps to match include:

- Organising the data received from Sumo to enable matching
- Ingesting the Sumo data into an enterprise analytic platform
- Conducting data matching activities which compare attributes of the supplied data against attributes stored in Medicare and Centrelink customer records
- Organising the matched records by confidence levels.

The data matching activities will involve the comparison of the following attributes supplied by Sumo against data stored in Medicare and Centrelink customer records:

- card number, expiry date and name appearing on Medicare or Centrelink card
- customer's date of birth
- customer's address.

The 'results' of the data match (i.e. where a successful match occurs) will contain the customer's name and an identity match score (known as a confidence level). Ratings for confidence levels are based on schema matching, e.g. name, gender, date of birth, address, phone number. The confidence level for an identity will be higher where more attributes are successfully matched.

Confidence levels are rated out of 10 with a score of 8 to 10 achieving high confidence.[2] When the total score achieves a high confidence level, an overall successful identity match is achieved.

Once a customer's identity has a high-confidence match, Services Australia will treat the customer's identity as compromised and will proceed to implement a series of protective measures for that customer.

5.2 Incorrect identity matches

Services Australia's data matching rules and techniques are constantly being refined to ensure risks are minimised. This is achieved by using the learnings of past and present data matching exercises.

Where an unconfirmed match occurs, a manual assessment is undertaken to attempt to resolve the issue. Unconfirmed matches include multi-matches, where the identity could relate to multiple agency records, and possible matches, where the identity match is not certain.

Where Services Australia determines that an unconfirmed match does not relate to any records held by Services Australia, the data will be deleted.

6. Action resulting from the program

Services Australia will assist affected customers in a number of ways to prevent and respond to identity fraud. Customers who have been notified by Sumo that their information has been compromised as a result of the Data Breach should have heightened awareness of suspicious or unexpected activity across all of their online accounts.

For each high level confidence match, Services Australia will apply proactive security measures on the impacted customer records. These measures will apply to:

- identify suspicious activity in relation to the customer's accounts, payment and services
- ensure Services Australia can respond quickly and appropriately.

Additionally, affected customer accounts will be monitored for possible future compromises.

[2] A score of 0 to 7 will be assigned a low confidence rating, on the basis that Services Australia cannot be genuinely satisfied that the identity belongs to an existing customer.

If these measures indicate suspicious activity, an investigation may also take place resulting in suspension/cancellation of payments. Suspension or cancellation activities would only occur where a customer account has been hijacked and action is required to protect the customer's identity and/or government outlays.

Services Australia does not propose to notify individual customers whose data is matched prior to taking action to apply security measures on the impacted customer records. As detailed in parts 4.1 and 5 above, Services Australia has processes in place to ensure the accuracy of information before taking administrative action. Where Services Australia proposes to undertake suspension/cancellation activities, Services Australia will contact the affected customer directly.

7. Time limits applying to the program

The data matching will be conducted after Sumo provides relevant customer data to Services Australia.

The data matching program will occur only once, unless further data is supplied by Sumo to Services Australia.

Services Australia will not create a permanent register or database of matched or non-matched data as part of this program.

In accordance with Guideline 7 of the Data Matching Guidelines, Services Australia will destroy:

- all data provided by Sumo which does not lead to a match
- all data matching results that do not achieve a high confidence match.

Otherwise, Services Australia will retain data obtained from Sumo and the records of matched data in accordance with the *Archives Act 1983* and *Privacy Act 1988*.

8. Public Notice of the program

The program protocol will be published on Services Australia's website. The program protocol along with any extensions of the program will also be notified in the Australian Government Gazette.

9. Reasons for conducting the program

9.1 Relationship with Services Australia's lawful functions

Services Australia is responsible for administering:

- Centrelink programs in accordance with the Social Security Act 1991 and the Social Security (Administration) Act 1999
- Medicare programs under the Human Services (Medicare) Act 1973, Health Insurance Act 1973 and National Health Act 1953.

The applicable legislative schemes provide eligibility criteria that must be met to enable various payments to be made. These requirements are given to payment recipients through written advice authorised under different sections of these Acts for different payment types. The success of the agency in administering Centrelink and Medicare programs is underpinned by the principle that only persons entitled to receive payments do so and receive correct entitlements. It is therefore paramount that Services Australia is well equipped to identify and respond to fraudulent activity arising as a result of the Data Breach.

9.2 Social Considerations

Centrelink and Medicare programs are often topical and of interest to the media and the public. There are some key social issues associated with each program including:

- ensuring those entitled to receive payments and services from the Services Australia do so and that they receive correct entitlements
- the desire of taxpayers to ensure integrity in Services Australia payments, services and recovery processes; and
- the protection of an individual's right to privacy, including identifying and taking steps to protect individuals who have been the victims of identity theft and minimising or preventing any further harm to those individuals.

In particular, there is strong support in the community for Centrelink and Medicare programs that directs available funds only to those who are eligible for assistance. The data-matching program helps to achieve this in two ways:

- through strengthening controls in Services Australia's payment systems, it reduces government outlays from the agency's programs, and
- the existence of effective controls in payment systems soon become evident to the community and rapidly increases voluntary compliance.

Suitable safeguards against unreasonable intrusion into the privacy of individuals are built into the data matching arrangements. Matching is conducted in accordance with the Data Matching Guidelines.

10. Legal authority

10.1 Services Australia

Services Australia has legal authority to match personal information and protected information:

- obtained from Sumo
- held in existing Centrelink and Medicare records.

Data obtained from Sumo

Data collected from Sumo will be personal information. As Services Australia will collect this personal information for the purpose of data-matching, the use of the data for the same purpose will be permitted under the *Privacy Act 1988*.

Additionally, data collected from Sumo will be protected information:

- under the *Social Security (Administration) Act 1999*, if information about a customer contains a Centrelink concession card number, expiry date and customer name
- under the *Health Insurance Act 1973* (and potentially the *National Health Act 1953*), if information about a customer contains a Medicare card number, expiry date and customer name.

As data matching will occur to identify and prevent abuse of the social security system and/or Medicare programs, the collection of personal information from Sumo is reasonably necessary for, or directly related to, one or more of the agency's functions or activities including the administration of social security law, performing functions in relation to a Medicare program, and preventing and detecting fraud. Exceptions to the protected information secrecy provisions will also apply to permit this matching, relevantly:

- section 202(2)(d) of the *Social Security (Administration) Act 1999*, which permits the use of protected information for the purposes of the social security law
- section 130(1) of the *Health Insurance Act 1973* and s 135A(1) of the *National Health Act 1953* which permit records to be made of protected information for the purpose of performing functions in relation to a Medicare program.

Data held by Services Australia

Similarly, while existing Centrelink and Medicare records will be protected information, the protected information provisions apply to permit the data-matching as it will occur for the purposes of the social security law and/or for the purpose of performing functions in relation to a Medicare program.

While data matching of Centrelink and Medicare records will occur for a different purpose for which the information was collected, APP 6.2(b) permits the secondary use of personal information where this is authorised by or under an Australian law. Data matching that is necessary for the purposes of the social security law and/or for the purpose of performing functions in relation to a Medicare program will engage the APP 6.2(b) exception.

10.2 Third Party Source

Services Australia considers that Sumo is authorised to provide information under section 86E of the *Crimes Act 1914*. This disclosure would occur to a target entity (Services Australia) for an integrity purpose. This disclosure would be authorised by law under APP 6.

11. Alternative Methods

Services Australia has several security measures in place to prevent and detect identity fraud in order to protect information and government outlays.

Services Australia runs an ongoing detection program designed to identify identity fraud conducted by individuals. In addition, the agency receives tip offs from the public in relation to identity fraud, however these tip offs are generally in relation to individuals or small groups.

Without this program, Services Australia has no mechanism to become aware of the large numbers of customers affected, or who may be affected, by the Data Breach. Using this program, information received from Sumo can be assessed and acted upon immediately.

12. Prior data match programs

No previous data matching programs exist in respect of this Data Breach.

13. Costs and Benefits

The benefits resulting from the program include enhanced data integrity through the assessment of mismatches and the continuation of Services Australia making appropriate payments and providing appropriate services to customers. This continued service to customers will provide assurance to customers whose data may have been compromised. This program will be delivered within existing agency resources.