Guidance note 11/02

Verification of identity: The use and disclosure of personal information by reporting entities and credit reporting agencies for the purposes of verifying an individual's identity – natural persons (e-verification)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

1. Background

1.1. Customer identification and verification of customer identity are key requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)*. The *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules) allows for document-based and electronic verification or a combination of the two. Where customer information is verified electronically, the verification must be based on 'reliable and independent electronic data'. The nature of the information which must be verified varies depending on whether the customer is a natural or legal person. Where the customer is a natural person the reporting entity must verify the customer's full name and either their date of birth or residential address.

1.2. Part 4.2 of the AML/CTF Rules also sets out a 'safe harbour' electronic verification process which may be used to verify the identity of customers who are natural persons when the reporting entity determines that the relationship with the customer is of medium or lower money laundering or terrorism financing risk. In these circumstances, paragraph 4.2.13 of the AML/CTF Rules specifies that the reporting entity should verify the following customer information:

a) name and residential address using reliable and independent electronic data from at least two separate data sources; and either
b) date of birth using reliable and independent electronic data from at least one data source; or
c) that the customer has a transaction history for at least the past three years.

1.3. Reporting entities, particularly those which operate online business models, have expressed strong interest in using electronic identity verification to meet their obligations under the AML/CTF Act. In practice, however, viability of electronic verification of identity is affected by the limited options available for using electronic-

based sources for confirming individual's details, in particular a person's date of birth.

1.4. Credit information files maintained by credit reporting agencies (CRAs) offer a reliable and independent source of information for the purposes of electronic verification of identity. The credit information files maintained by the larger CRAs include date of birth and other relevant information on most of the adult population of Australia. However, sections 18K and 18L of the *Privacy Act 1988* (Privacy Act) place detailed limits on the disclosure of personal information held by CRAs and the use of information in credit reports by credit providers, and to date have precluded the use of personal information held on an individual's credit information file for the purposes of electronic verification of identity under the AML/CTF Act.

1.5. The Australian Law Reform Commission considered the question of the use of credit reporting information for electronic verification in its inquiry For Your Information: Australian Privacy Law and Practice (2008). The ALRC recommended that, provided appropriate privacy protections were implemented, 'the use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the [AML/CTF Act] should be authorised expressly under the AML/CTF Act' (Recommendation 57-4). The Government agreed in principle to the recommendation and subsequently undertook a Privacy Impact Assessment (PIA) to investigate appropriate privacy protections. Affected private sector businesses and peak bodies, and privacy groups were consulted as part of the PIA process. The outcomes of the PIA informed the development of the e-verification provisions now found in Division 5A of Part 2 of the AML/CTF Act.

1.6. In summary the e-verification provisions:

- permit a reporting entity to disclose specified personal information to a CRA for identity verification purposes with the express consent of the individual whose identity is being verified
- permit a CRA to conduct a matching process between personal information provided to it by a reporting entity and the personal information held on its own files and provide an assessment to the reporting entity of the outcome of the verification process
- require reporting entities to notify their customers, or other individuals required to be identified under the AML/CTF Act of unsuccessful attempts to verify identity using credit reporting data
- require credit reporting agencies and reporting entities to retain information about verification requests and assessments for 7 years from the date of the request for CRAs and for 7 years after ceasing to provide designated services to a customer for reporting entities and to delete it at the end of those periods
- require a CRA to keep information about verification requests separate from the individual's credit information file
- create offences to address unauthorised access to, and disclosure of, verification information.

2. Introduction

2.1. The purpose of this guidance note is to assist reporting entities to understand the provisions in Division 5A of Part 2 of the AML/CTF Act which permit reporting entities to verify an individual's identity, through matching specified personal information provided to a reporting entity by the customer, or other individual the reporting entity is required to identify, to records held by a CRA.

2.2. The use of personal information contained in a credit information file is limited to verification of identification information for customers, or other individuals the reporting entity is required to identify, who are natural persons.

2.3. Division 5A of Part 2 of the AML/CTF Act authorises the use and disclosure of personal information contained in a credit information file by and between a reporting entity and a CRA for the purpose of verification of identification information, which overcomes the prohibition set out in Part III of the Privacy Act. This new method of verification is permitted by amendments to the AML/CTF Act and the Privacy Act.

3. Electronic verification of customer identity

Reporting entities

3.1. Reporting entities are permitted to:

- Disclose the identification information – specifically, one or more of an individual's name, residential address and date of birth – to a CRA (subsection 35A(1) of the AML/CTF Act).
    - Transaction history is not permitted to be used in relation to this method of verification.
- Use the assessment provided by the CRA, which indicates whether the identification information provided by the reporting entity matches the information held by it on its credit information files, to verify a customer's or other individual's identity for the purposes of the AML/CTF Act.
    - As the assessment from the CRA must contain an aggregate score or ranking to indicate the level or degree of match of the information, reporting entities will need to determine, in conjunction with their risk analysis under their AML/CTF program, whether a CRA's assessment will be considered sufficient for verification of the identity of the individual.

3.2. Reporting entities are required to:

- obtain express and informed consent from an individual, as set out in section 35A (2) of the AML/CTF Act, prior to making a verification request:
    - The concept of express consent is not defined in the Privacy Act. For the purposes of this Guidance Note, it means that the individual must actively agree to a reporting entity verifying their identity against personal information held by a CRA. A reporting entity cannot rely on implied consent (where agreement is taken to have occurred based on the absence of evidence of disagreement).

- Express consent can be indicated online, or on the phone. However, records must be retained to evidence the process followed and the consent given by the individual.

An example of express consent in an online context is that a customer may be required to 'check' a box indicating that the customer has read the information and consents (active). A reporting entity could not rely on a failure to opt out (passive – eg. customer did not 'uncheck' an automatically checked box) to indicate consent.

- To ensure that the consent is informed, the consent must be specifically about the disclosure of personal information by the reporting entity to the CRA and use by the CRA of the personal information contained in credit information files for an assessment. The consent will specify that the reporting entity will only use the assessment by the reporting entity for the purpose of verifying the individual's identity for the purposes of the AML/CTF Act: a general consent to the use of information to verify identity will not be sufficient. If an individual other than the customer is being identified, that person will also have to consent to the process.

The individual must be given information about: - the reason for making the request for verification, - the personal information that may be provided to the CRA, and - the fact that the reporting entity is seeking, and the CRA may provide an assessment of whether the personal information matches (in whole or in part) information on the individual's credit information file.

- To ensure that the consent is genuine, paragraph 35A(2)(c) requires that the individual must be given another option, not reliant upon credit reporting information, for verifying their identity. This will ensure that those who choose not to use their credit information file for this purpose, or those who do not have a credit information file, are not disadvantaged when seeking to obtain designated services.

- notify the individual of a failure to verify the information in a written notice, if the assessment from the CRA does not enable the reporting entity to verify an individual's identification information, as set out in section 35C of the AML/CTF Act.
  - Paragraph 35C(2)(b) specifies that the written notice must contain the details of the CRA that provided the assessment which resulted in the failure to verify. This enables the individual to make their own direct inquiries with the CRA concerning the accuracy of the information contained on their credit information file. Sections 18H and 18J of the Privacy Act provide rights of access and alteration for individuals relating to their credit information file or credit reports held by CRAs and credit providers.
  - Paragraph 35C(2)(c) requires that the individual be given another means of verifying their identity. This ensures that an individual is not denied a designated service based on the assessment of the CRA alone. This provides additional protection for individuals in circumstances where the

information held by the CRA is not accurate, resulting in a low match assessment.
    - Written notice includes a notice delivered electronically, such as by email.
- retain a record containing specified information relating to a verification request. As set out in section 35F of the AML/CTF Act, a reporting entity must retain this information for a period starting from the date of the verification request and ending 7 years after the reporting entity ceased providing a designated service to the individual, and must delete it at the end of that period. This retention period is consistent with other record keeping obligations under the AML/CTF Act, and will enhance the level of transparency of the verification processes by ensuring that records can be reviewed to ensure compliance with the relevant requirements and to enable individuals to obtain access to verification requests and the outcomes of any assessments.

The record must contain:
- the name of the CRA to which the request was made,
- the personal information provided to the CRA,
- the assessment received, and
- any other information specified in the AML/CTF Rules.

At this stage, no additional information is specified in the AML/CTF Rules.

Designated Business Groups

Subsection 35F(5) of the AML/CTF Act allows any member of a designated business group (DBG) to discharge the obligation regarding retention of these records for another member of the DBG.

Credit Reporting Agencies

3.3. A CRA is permitted to:

- use the personal information about the individual, provided by the reporting entity, and the personal information in its credit information files, for the purposes of assessing whether the information matches (in whole or in part).
    - Subsection 35B(1) enables a CRA to prepare an assessment for a reporting entity (or its authorised agent) on whether the personal information it was provided matches the information held on its credit information file.
    - A CRA will undertake a simple matching process with any or all of the individual's name, residential address and date of birth. It cannot consider any other details or aspects arising from the individual's credit information file beyond those details that correspond with the information provided by the reporting entity.
    - Paragraph 35B(1)(b) recognises that it may be necessary for a CRA to also have regard to information that is held on other individuals who have similar identifiers in order to undertake an effective matching process so

the CRA may rule out other similar but non-matching persons. Therefore, a CRA may use both the personal information about the individual and the names, dates of birth and residential addresses of other persons for the purposes of providing an assessment for a reporting entity.

- provide, as a response to a request to verify identification information, an assessment report on whether the personal information provided by the reporting entity matches information that it holds on its credit information file.
    - A CRA is not permitted to disclose any information from the individual's credit information file, other than the assessment of whether the information supplied matches information on file.
    - A CRA is not permitted to use the information supplied by the reporting entity for the purposes of verification for any other purpose, for example, as part of the assessment of a person's credit worthiness.

Content of assessment report

3.4. As set out in subsection 35B (2), the CRA can only provide an overall assessment of the match between personal information. The CRA cannot provide a separate assessment of the match between particular categories of personal information, that is, the individual's name, date of birth and residential address.

- It is expected that in practice a CRA will provide an overall assessment in verifying the individual's identity by using either an aggregate score or ranking system in reporting the outcomes of the matching process.
- The intention behind the use of an aggregate match is to minimise the potential for misuse or attempts by criminal elements to use a trial and error approach to matching identity with false names or stolen identities.

For example, if a CRA has identified a complete match to the information provided on an individual by a reporting entity, it will either report a "Complete Match" or provide a score – "100 percent match" or something similar.

Using this same example, if the CRA does not have a complete match, it may report it as a "Strong Match" or "90-99 percent match".

If there is an incomplete match, it may be reported as a "Partial Match" or "50 percent match".

This graded response will continue through the various levels to situations where there is no match.

3.5. A CRA is required to:

- retain a record of specified information relating to a verification request for a period of 7 years after the request was received, and must delete it at the end of that period. This obligation, set out in section 35E of the AML/CTF Act, will enhance the level of transparency of the verification processes by ensuring that records can be reviewed to ensure compliance with the relevant requirements and to enable individuals to obtain access to information regarding verification requests against their credit information file.

This record must contain:
- the name of the reporting entity that made the request,
- the date of the request,
- the personal information provided to the CRA,
- the date on which an assessment was provided in relation to the request, and
- any other information specified in the AML/CTF Rules.

At this stage, no additional information is specified in the AML/CTF Rules.

- keep information about verification requests separate from the individual's credit information file. Section 35D of the AML/CTF Act states that a CRA is prohibited from including on an individual's credit information file personal information which relates to a verification request or assessment conducted in relation to the individual.
    - This overrides the requirement in subsection 18K(5) of the Privacy Act, which requires a CRA to make a file note of any disclosure involving personal information contained in an individual's credit information file.

Enforcement provisions

3.6. The use of credit reporting information for identity verification purposes is underpinned by strong offence provisions to deter inappropriate conduct:

- The offences include unauthorised access to verification information, obtaining access to verification information using false pretences, and unauthorised use or disclosure of verification information (at ss35H, 35J and 35K respectively). Each offence carries a penalty of 300 penalty units (currently $33,000).

3.7. In addition, a breach of the requirements of Division 5A of the AML/CTF Act is an interference with the privacy of an individual, granting the Australian Information Commissioner jurisdiction to investigate alleged breaches (section 35L).

Individual's rights

3.8. An individual has the right to:

- Choose whether to agree to verification using information held on their credit information file (section 35A of the AML/CTF Act).
- Be advised if a verification attempt is unsuccessful (section 35C of the AML/CTF Act), including details of which CRA was involved, and offered an alternative means of verification.
- Access information relating to verification requests from the reporting entity and from the CRA (section 35G of the AML/CTF Act).
- Lodge a complaint with the reporting entity or CRA if they believe that their information has not been handled in accordance with the requirements set out in these provisions, and lodge a complaint with the Office of the Australian Information Commissioner if the complaint is not resolved by the reporting entity to the individual's satisfaction.

4. The Privacy Act and the Office of the Australian Information Commissioner

4.1. The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency established by the *Australian Information Commissioner Act 2010* (AIC Act). The agency commenced operation on 1 November 2010 and is headed by the Information Commissioner, supported by two other statutory office holders, the Freedom of Information Commissioner and the Privacy Commissioner. Staff of the former Office of the Privacy Commissioner (OPC) are now part of the OAIC.

4.2. The Commissioners of the OAIC exercise the privacy functions set out in s 9 of the AIC Act. These include functions outlined in the *Privacy Act 1988* (Cth) (Privacy Act) itself. Section 28A of the Privacy Act confers functions in relation to credit reporting such as investigations of credit infringements by credit providers and credit reporting agencies (CRAs); audits of credit information files and reports; and advice and guidance to relevant parties.

4.3. The Privacy Act regulates the handling of personal information by the Australian Government, the ACT Government and the private sector. The Act includes 10 National Privacy Principles (NPPs) that apply to most private sector organisations and Part IIIA which applies to credit reporting agencies and credit providers. The NPPs establish, for certain private sector organisations including all reporting entities, obligations relating to personal information, including in relation to collection, use and disclosure, accuracy, storage, and a person's right to access information held about them. Part IIIA includes specific provisions relating to credit information files.

4.4. To assist organisations to understand their obligations under the Privacy Act, the Office of the Australian Information Commissioner has developed a set of guidelines on the National Privacy Principles (NPPs),

Legal authority for disclosure of personal information by a reporting entity

4.5. National Privacy Principle 2 of Schedule 3 of the Privacy Act regulates the use and disclosure of personal information by relevant private sector organisations. The National Privacy Principles (NPP) can be located at the link above. Paragraph 2.1 of NPP 2 provides the following:
"2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection…"

4.6. There are a number of exceptions to this obligation, and in particular, paragraph 2.1 (g) of NPP 2 states the following exception:
"(g) the use or disclosure is required or authorised by or under law"

4.7. Subsection 35A(3) provides that disclosure of personal information by a reporting entity in accordance with paragraph 35A(1)(a) is taken to be authorised by law for the purposes of NPP 2.1(g).

Legal authority for disclosure of personal information by a CRA

4.8. The Privacy Act, at s18K(1), prohibits a CRA from disclosing personal information contained on a person's credit information file, unless one of the exceptions applies.

Subparagraph 18K(1)(m) provides an exception when the disclosure is required or authorised by or under law.
Subsection 35B(3) of the AML/CTF Act specifically states that the provision of an assessment report to a reporting entity in response to a request for verification is a disclosure authorised by law for the purposes of paragraph 18K(1)(m) of the Privacy Act.

Further information

AUSTRAC officers are able to assist reporting entities, their staff and the public in providing general information relating to the AML/CTF Act. Enquiries can be directed to the AUSTRAC Contact Centre via:

email to help_desk@austrac.gov.au
telephone 1300 021 037 (a local call within Australia).

The information contained herein is current as at the date of this document.

Reporting entities should note that in relation to activities they undertake to comply with the AML/CTF Act, they will have obligations under the *Privacy Act 1988*, including the requirement to comply with the Australian Privacy Principles, even if they would otherwise be exempt from the Privacy Act. For further information about these obligations, please refer to the Office of the Australian Information Commissioner or call 1300 363 992.

July 2011

Australian Transaction Reports and Analysis Centre (AUSTRAC)
PO Box 5516
West Chatswood NSW 1515

Telephone: 1300 021 037
Facsimile: 02 9950 0071
Website: AUSTRAC
Email: help_desk@austrac.gov.au