# Submission to the Senate Committee on Constitutional and Legal Affairs Anti-Money and Counter-Terrorism Financing Bill 2005 ("AML/CTF Bill")

## Electronic Verification Procedures

### 1. Principles for customer verification

AUSTRAC has indicated that in the case of a natural person, only the name, date of birth and current residential address of a person will need to be verified under the "*applicable customer identification procedure*" to be set out in the AML/CTF Rules.

### 2. Issue: Electronic verification

At this stage, electronic verification is not provided for in the draft AML/CTF Rules. GE considers that electronic verification should be expressly permitted.

### 3. What is electronic verification and how is it relevant to customer identification?

The identification of a customer consists of:

(a) **(identification)** collecting information about a customer (in the AML/CTF Bill and the draft Rules, this is referred to as the "*minimum KYC information*"); and

(b) **(verification)** verifying or confirming the information that the customer has given so that a reporting entity can be satisfied that the customer is who they say they are.

Electronic verification is the process of verifying customer information by carrying out checks of electronic databases that store information about people (eg the electronic versions of White Pages and Yellow Pages, and credit reporting agencies such as Baycorp). It may be performed by the reporting entity itself, or a third party service provider and is just one method of verifying the identity of a customer.

### 4. Recommendation

GE recommends that the electronic verification procedure set out in the Schedule to this submission be included in the AML/CTF Rules.

### 5. Submissions in support of the Recommendation

GE considers that the Recommendation is appropriate to address the issue and should be included in the AML/CTF Rules because:

(a) **(FATF)** it is consistent with the FATF Recommendations because it only permits electronic verification where reliable data sources are used[1];

(b) **(AUSTRAC)** it is consistent with AUSTRAC's view that an electronic verification procedure should be robust because:

- the reporting entity would be required to make assessments of reliability and accuracy of a proposed electronic verification procedure as part of its obligation to implement AML/CTF programs; and
- AUSTRAC has, as recently as July 2005, approved at GE's request (as permitted by the Financial Transaction Reports Act 1988) an alternative customer identification procedure that includes a substantially similar electronic verification procedure to that set out in the Recommendation;

(c) **(UK)** it is not inconsistent with the approach in the United Kingdom[2];

(d) **(efficient)** it enables reporting entities to perform the applicable customer identification procedure efficiently and as quickly as possible, with minimal disruption to the reporting entity's business;

(e) **(certainty)** it will avoid ambiguity or uncertainty as to whether and what form of verification will satisfy a reporting entity's obligation to perform the "*applicable customer identification procedure*";

(f) **(technology neutral)** it is technology neutral, as agreed at the third financial services industry Round Table meeting convened by Senator Ellison and is consistent with the Commonwealth Government's general approach to e-commerce (eg, as under the Electronic Transactions Act 1999); and

(g) (**channel neutral**) there is no obvious reason why electronic verification should be confined to circumstances where a designated service is provided in a non face-to-face situation as currently contemplated by the Draft Guidance Paper on Applicable Customer Identification Procedures ("**Draft Paper**")[3], a distinction not contemplated by the FATF Recommendations or the UK approach.

[1] See paragraph (a) of FATF Recommendation 5.
[2] See the Joint Money Laundering Steering Group's "*Prevention of money laundering / combating the financing of terrorism: Guidance for the UK Financial Sector, Part I*" (January 2006) ("**Guidelines**") and the draft notes in the Schedule.
[3] See paragraph 14.

# Schedule - Recommendation

["**Applicable Customer Identification Procedure**

X. The applicable customer identification procedure consists of:

(a) obtaining the minimum KYC information about a customer; and

(b) confirming, or verifying, the identity of the customer on the basis of the minimum KYC information."]

*[Drafting Note: The Applicable Customer Identification Procedure rules should make it clear that the procedure consists of these two distinct processes. Separate rules should be drafted for the verification process contemplated by (b). The verification process should consist of at least two options for verification. A standard verification process (eg confirming identity using documents such as passports) and the electronic verification process as set out below. The verification processes should apply as options regardless of the method used to collect the minimum KYC information and regardless of whether a designated service is provided face-to-face. This approach is consistent with the UK approach - see the drafting notes below.]*

"**Electronic verification of customer identity**

1. Reporting entities may use technology solutions to verify a customer's identity electronically. If a reporting entity uses electronic verification methods, the method must use reliable, independent source documents, data or information.

2. A service provider that provides electronic data services may be used by a reporting agency to electronically verify identification. If a reporting entity uses such services, it must be satisfied that the service provider provides information that is reliable and accurate.

3. In assessing whether the electronic data services of a service provider are reliable and accurate, the reporting entity should have regard to:

(a) the service provider's compliance with laws relating to privacy and the collection of personal information;

(b) the range of data sources (including commonwealth, state or local government controlled records and registers) that it uses and the methods it uses to collate and provide information;

(c) the transparency of the processes used by the service provider and any reports that it is able to give a reporting entity on the searches it has conducted; and

(d) the means by which the service provider evaluates the reliability and accuracy of the electronic data it provides.

*[Drafting Note: This is based on the UK criteria for use of an electronic data provider as set out in paragraphs 5.3.17 to 5.3.18 of the Guidelines.]*

4. The minimum KYC information that should be used as a base for electronically verifying a natural person's identity (including a customer who is operating as a corporation sole) is:

   (a) the customer's full name;

   (b) the customer's full residential address; and

   (c) the customer's date of birth.

*[Drafting Note: The information extracted in paragraphs 4, 5 and 6 have been extracted from the minimum KYC information proposed by the Draft Identification Rules that have been publicly released. The select minimum KYC information that has been suggested as forming the base for enquiries as part of the electronic verification process is similar to that which is recommended in the Guidelines at paragraph 5.4.23 for the electronic verification in the UK.]*

5. The minimum KYC information that should be used as a base for electronically verifying the identity of a company is:

   (a) the full name of the company;

   (b) the full address of the company's principal place of business;

   (c) the ABN or ARBN of the company; and

   (d) the name of the country in which the company was incorporated.

6. The minimum KYC information that should be used as a base for electronically verifying a identity of non-natural person who is not a company is:

   (a) the full name of the legal person [who opened the account];

*[Drafting Note: The words "who opened the account" is from the draft minimum KYC information, but we suggest that this is too narrow, having regard to the definition of designated services.]*

   (b) the business name (if any) under which the customer carries on, or proposes to carry on, business or activities;

   (c) the full address of the customer's principal place of business full residential address; and

   (c) the customer's date of birth.

7. An electronic verification procedure should not be accepted by the reporting entity as reliable and accurate unless the reporting entity is satisfied that the procedure satisfies a minimum level of electronic verification. The minimum level of electronic verification that reporting entities should use is an exact, strong or possible match against 2 or more of the minimum KYC information specified in paragraphs 4, 5 or 6 (as applicable in the circumstances).

*[Drafting Note: The Guidelines recommend a standard level of confirmation to assess whether the verification process has resulted in confirmation of the customer's identity. See paragraph 5.4.24 of the Guidelines.]*

8. The reporting entity should verify any one or more of the minimum KYC information not specified in paragraphs 4, 5 or 6 (as applicable in the circumstances) to mitigate against the risk of impersonation fraud. The additional check may consist of measures that the reporting entity routinely takes or another measure that is established by the reporting entity for that purpose.

*[Drafting Note: The Guidelines (see paragraphs 5.4.25, 5.4.31 and 5.4.32) suggest that reporting entities should mitigate against the risk of impersonation and sets out examples by which this may be achieved. We suggest that examples not be included in the AML/CTF Rules because of the risk that this may limit the scope of measures that reporting entities will consider to manage this risk. It is therefore preferable to state the obligation and for businesses to then consider the money laundering and terrorist financing risk that arise in their business and to implement processes accordingly. Examples could, however, be described in any proposed guidance paper.]*

*[Other Drafting Notes:*

- *This Recommendation is based on the Draft Paper. To the extent that changes are made to the Draft Paper as a result of the consultation process (for example, to the minimum KYC information), the Recommendation may need to be adjusted to take account of those changes.*

- *The Recommendation has been drafted on the basis that it is one option for carrying out the second phase of the identification process. As such, electronic verification is not a mandatory procedure. References to the word "should" are therefore to be construed as indicating a way in which the applicable customer identification procedure may be satisfied.*

- *The Recommendation assumes that no changes will be necessary to the Privacy Act 1988 (Cwth) to permit electronic verification on the basis that the use or disclosure of the minimum KYC information is authorised by or under law[4].]*

[4] See National Privacy Principle 2.1(g).