cancelled, forged, tampered with or stolen and, if so, what steps the reporting entity will take to establish whether or not the document has been cancelled, forged, tampered with or stolen;

(5) whether the reporting entity will use any authentication service that may be available in respect of a document; and

(6) whether, and how, to confirm information about a customer by independently initiating contact with the customer.

Part 4.10 Verification from reliable and independent electronic data

4.10.1 In so far as an AML/CTF program provides for the verification of KYC information collected about a customer by means of reliable and independent electronic data, an AML/CTF program must comply with the requirements specified in paragraph 4.10.2.

4.10.2 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine:

(1) whether the electronic data is reliable and independent, taking into account the following factors:

(a) the accuracy of the data;

(b) how secure the data is;

(c) how the data is kept up-to-date;

(d) how comprehensive the data is (for example, by reference to the range of persons included in the data and the period over which the data has been collected);

(e) whether the data has been verified from a reliable and independent source;

(f) whether the data is maintained by a government body or pursuant to legislation; and

(g) whether the electronic data can be additionally authenticated; and

(2) what reliable and independent electronic data the reporting entity will use for the purpose of verification;

(3) the reporting entity's pre-defined tolerance levels for matches and errors; and