THE TA FORUM
AML Working Group

Electronic identification standards/configuration for Online Account Opening

The standard for electronic verification, whether used for traditional *paper-based application form* account opening or as an integral part of an online account opening solution, is set out in JMLSG Part I[1].

Fundamentally, and consistent with JMLSG 5.3.52, before using a commercial organisation for electronic verification of identity, firms should be satisfied that the information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate, and independent of the customer.

Firms should therefore be satisfied that the use of an electronic verification tool meets the standard envisaged by JMLSG i.e.

- the provider is recognised through registration with the Information Commissioner's Office ("**ICO**");
- if the provider is not on the ICO's list of credit reference agencies, it is accredited/certified to offer an identity verification service that involves meeting minimum published standards;
- the service uses a range of multiple, positive information sources;
- the service accesses negative information sources such as Sanctions and PEP data or mortality records, for example;
- through its published standards, the provider undertakes to keep data up-to-date, or maintained within defined periods of re-verification;
- the provider's standards are assessed/audited; and
- transparent processes are used to enable firms to understand the checks carried out, the results returned and the certainty such results provide to evidence 'living as stated'.

To ensure continued suitability, firms should ensure the provider is capable of providing an annual attestation to support the foregoing criteria. Accordingly, such capability should be acknowledged either as a contractual clause, or as a confirmed Service Level Agreement standard. If a provider cannot guarantee to provide such an attestation, firms should consider the regulatory and reputational implications that may arise before entering into a service contract.

[1] Chapter 5 paragraphs 5.3.39 – 5.3.53

Where online account opening services are provided, firms must ensure T&Cs or other essential customer document(s) inform applicants that their personal details may be submitted for e-verification both at the outset of the relationship and at various points of the business relationship, to ensure compliance with the Data Protection (and GDPR when it comes into force).

Best practice suggests firms should take a risk-based approach to e-ID failures. Where high risk failures are returned because, for example, an applicant is name matched to a Sanctions target, the online process should **hard-stop** and the applicant invited to contact the management company for further information/instruction.

Where e-ID fails because there is insufficient electronic evidence to create a meaningful *footprint*, firms should allow the online account opening to conclude, with system functionality designed to capture the failure, whilst simultaneously informing AML Compliance and relevant Operational teams, thereby allowing actions to be taken to gather traditional paper-based evidences to satisfy the requisite customer verification standard. Again, T&Cs etc. should make clear customers may be required to provide such paper-based evidences and failure to provide may result in cancellation of business etc.

Key points, therefore, are:

- an appropriate e-ID tool to the requisite JMLSG standard;
- integrated system functionality, informing processes, including hard-stop;
- DPA compliant customer disclosures explain e-verification will be used;
- firms to retain the right to gather paper-based evidences where required; and
- firms' ability to gather annual attestations.