THE TA FORUM
AML Working Group

Verification of the Vulnerable

THE TA FORUM
AML Working Group

Contents

THE TA FORUM
AML Working Group

Introduction

The generally accepted definition of a vulnerable person is someone who is either a minor (with whom TA Forum members would be unlikely to deal) or an individual who, for physical or mental health reasons, may not be able, *inter alia*, to look after their personal finances and who may have little or no standard evidence available to immediately meet requests to enable the effective discharge of *know your customer* responsibilities.

Unless vulnerability is made clear at the outset of a relationship, or intra relationship, identifying a vulnerable person can be challenging and fraught with subjectivity. One person's assessment may differ entirely from that of another. This paper therefore seeks to determine ways in which firms may be able to verify vulnerable persons in line with legislation and JMLSG Guidance.

As 'minors' will not be directly invested, the focus is therefore on the 'vulnerable adult', the statutory definition of which is a person over the age of eighteen, towards who the state has specific safeguarding responsibilities, such as[1]:

- living in residential or sheltered accommodation;
- receiving certain types of health and social care;
- receiving certain types of welfare support;
- detained in lawful custody;
- older people who are physically or mentally frail;
- people with learning disabilities;
- people with a mental health condition such as dementia or personality disorder;
- people who are ill and need help to carry out normal daily functions;
- people with physical disabilities;
- people who have undergone a recent trauma e.g. bereavement, divorce or job loss; or
- people who may be in abusive relationships or are homeless.

Verification of the individual will, of course, depend on the nature of the product or service requested.

Acknowledging the difficulties presented by determining vulnerability, no exhaustive list can be defined. However, **vulnerability indicators** may present as:

- a decision that is unusual, unexpected or out of character;
- a close friend, relative, carer or clinician may highlight a concern;
- applications, transactions and/or contract notes may not be understood; or inability to understand the information and explanations provided in written or telephone communications.

[1] The list is not exhaustive with the full criteria being available in Safeguarding Vulnerable Groups Act 2006,

Verification of the Vulnerable

Where appropriate, firms should seek to verify a vulnerable person in line with JMLSG's standard requirements for private individuals[2], applying a risk-based approach as appropriate.

Electronic verification should be considered initially to validate the individual if the product meets the requirements envisaged by JMLSG. However, caution, and therefore reduced expectation, should be exercised and applied given the potential that such individuals may not possess the breadth and depth of electronic data to create a meaningful footprint.

Should electronic verification be unsuccessful, firms should seek 'traditional' standard paper-based evidences in certified copy (preferably) or original form; recognising, as noted above, that documents may be limited in number thereby creating verification constraints. Should this be the case, firms must consider what other documents[3] may be available and which might be produced from reliable and independent sources sufficient to discharge the requisite responsibility under the regulatory system.

As firms are required to compensate for difficulties individuals may have when asked to provide standard evidence of identity, a reasonable approach should be adopted to verify the individual. Further, SYSC 6.3.7(5) states firms should ensure systems and controls include:

"appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity".

The FCA Rules on financial exclusion will be apparent in some cases but where members identify and document an individual cannot reasonably meet the standard verification requirements; consideration should be given to gathering evidences from the following sources[4]:

- DWP entitlement Letter;
- HMRC or local authority entitlement letter;
- Identity Confirmation Letter issued from either the DWP or local authority;
- Letter from a care home manager/warden of sheltered accommodation or refuge; or
- Solicitor's letter or equivalent confirming identity verification.

Where firms identify an applicant or beneficial owner as vulnerable or one who does not have the capacity to manage their financial affairs or if they are informed a person is losing or lacking capacity, firms should document the finding or notification accordingly. However, notifications without evidence should be treated with caution given the potential that such notice might be vexatious and open to challenge should the named individual not be suffering some form of incapacity. Ultimately, it is essential that firms obtain evidence of any authority to act, in addition to having appropriate systems

[2] JMLSG Part I Chp 5 5.3.71 on
[3] In line with Regulation 28(18)b
[4] JMLSG Part II, sector 1; Retail Banking.

and controls to identify potential financial exploitation, which is, sadly, an inevitable consequence prevalent in vulnerability cases.

Where appropriate, further verification methods should include obtaining:

- original or certified Power of Attorney documents[5];
- original or certified Court of Protection Order[6]

Where a Lasting Power of Attorney is provided, firms should follow and document validity in line with the Office of the Public Guardian's requirements. Court of Protection validation requirements will follow similar requirements.

Where an account is taken-over by a personal representative, firms should ensure they have in place the appropriate framework to document each appointment.

Firms may also rely on introducer certificates from regulated intermediaries authorised on the account, or from professional persons known to the investor, verification can consist of:

- Confirmation of Verification of Identity Certificate (CVI);
- Letter on headed paper confirming evidence and verification in line with JMLSG; or
- Solicitor's Letter or equivalent confirming verification of identity.

It is important to document where reliance has been placed and evidenced in line with a firm's policy.

Mitigation of impersonation risk

Non-face-to-face verification can increase the fraud risk with authentication dependent on a firm's risk assessment. Therefore, where appropriate, additional measures should be applied to mitigate such risk. Examples of mitigation techniques may include:

- Payment to the source account, where a clear record of same is available from customer on-boarding;
- Payment to a new account held in the name of the customer, but care of an Attorney or similar, with appropriate evidences gathered to enable this to be achieved; or
- Independent clarification with the named attorney(s) subject to satisfactory verification having first been established.

[5] Attorneys to be verified to JMLSG standard
[6] Deputies or similar to be verified to JMLSG standard

Vulnerability should be treated with caution. It should not be left to individual members of staff to determine outcomes unilaterally where there is any doubt or concern. Instead, recommendations should be tabled and agreed outcomes determined, including engaging with the relevant Manco where same is considered appropriate or SLAs demand such interaction. At all times, a written record of all such decisions must be made and retained.