JMLSG Guidelines for Electronic AML Verification

The Joint Money Laundering Steering Group sets out comprehensive guidelines for practitioners to follow to conform to UK AML Legislation.

These are the relevant segments of the regulations that are relevant for electronic AML verification and how AML checks through Searchpoint and in particular our service partner GBGroup meets them.

Criteria for Electronic AML Checks

"*For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity.*" (*JMLSG Guidelines 2009 Section 5.3.38)*

"*The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:*

- *One match on an individual's full name and current address,* ***and***
- *A second match on an individual's full name and* ***either*** *her/his current address* ***or*** *his date of birth" (JMLSG Guidelines 2009 Section 5.3.80)*

The criteria for creating a PASS in JMLSG criteria is a 2+2 or in other words it has to match 2 names to 2 addresses OR 1 name to 1 address AND 1 name to 1 Date of Birth.

A 2+2 pass can be achieved through:

- Verifying an individual to an address by surname and forename on two separate databases

OR

- Verifying an individual to an address by surname and forename on one database & verifying an individual by forename, surname and date of birth.

Mitigation of impersonation risk

There are additional requirements for JMLSG, two of which are mentioned below as they also affect Electronic Verification:

"Where identity is verified electronically, or copy documents are used, a firm should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- *requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from an equivalent jurisdiction;*
- *verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.3.25);*
- *telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;*
- *communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);*
- *internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;*
- *other card or account activation procedures;*
- *requiring copy documents to be certified by an appropriate person." (JMLSG Guidelines 2009 Section 5.3.82)*

Politically Exposed Persons (PEPs) & Sanctions Lists

There are many bodies that provide Sanctions Lists and PEP Lists throughout the world including HM Treasury, European Union, Home Office, United Nations and US Department of State.

Searchpoint use the C6 Database which covers data from 240 countries and is widely regarded as the most comprehensive coverage available.

International pressure to have effective AML/CTF procedures

"*The United Nations and the EU have sanctions in place to deny a range of named individuals and organisations, as well as nationals from certain countries, access to the financial services sector. In the UK, HM Treasury issues sanctions notices whenever a new name is added to the list, or when any details are amended*." *(JMLSG Guidelines 2009 Section 1.9)*

Nature of electronic checks

"*A number of commercial agencies which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list. Some of these sources are, however, only available to closed user groups*. *"(JMLSG Guidelines 2009 Section 5.3.35)*

Persons firms should not accept as customers

"*The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions, in accordance with legislation explained below. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. A Consolidated List of all targets to whom financial sanctions apply is maintained by HM Treasury, and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at: www.hm-treasury.gov.uk/financialsanctions. "(JMLSG Guidelines 2009 Section 5.3.41)*

The obligations under the UK financial sanctions regime apply to all firms, and not just to banks. The Consolidated List includes all the names of designated persons under UN and EC sanctions regimes which have effect in the UK. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although a firm doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. The other websites referred to below may contain useful background information, but the purpose of the HM Treasury list is to draw together in one place all the names of designated persons for the various sanctions regimes effective in the UK. All firms to whom this guidance applies, therefore, whether or not they are FSA-regulated or subject to the ML Regulations, will need either:

- *for manual checking: to register with the HM Treasury update service (directly or via a third party, such as a trade association); or*
- *if checking is automated: to ensure that relevant software includes checks against the relevant list and that this list is up to date.*

(JMLSG Guidelines 2009 Section 5.3.42)

Customers other than private individuals

"*Where an entity is known to be linked to a PEP (perhaps through a directorship or shareholding), or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher risk category, and that enhanced due diligence measures should therefore be applied (see sections 5.5 and 5.7*). *(JMLSG Guidelines 2009 Section 5.3.118)*

Politically exposed persons (PEPs)

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. *(JMLSG Guidelines 2009 Section 5.5.18)*

http://www.searchpoint.co.uk/anti-money-laundering/

TC/30/06/2015