Anti-Money Laundering Guidance Note – Identification and verification during COVID-19

Undertaking the appropriate level of client due diligence (CDD) is a statutory requirement that continues to apply during COVID-19. However, the money laundering regulations[i] (MLRs) provide the flexibility to identify and verify your clients digitally, allowing you to adhere to the Government's advice on social distancing during the COVID-19 pandemic.

This Guidance Note summarises previous guidance from the CLC and the Legal Sector Affinity Group (LSAG) advice on identification and verification (ID&V). While you are not able to meet clients in person and view physical identify documents, consider using alternative digital ID&V methods that provide you with enough assurance that a client is who they claim to be. These methods could also be useful for your firm and clients even after social distancing requirements are relaxed.

Remember:

- Always adopt a risk-based approach in determining the level of CDD you apply.
- Update your policies, controls, and procedures and keep a record and evidence of the processes you follow for ID&V (for example of any video calls made) and decisions you make.
- When updating records for existing clients do not rely on ID provided previously just because you cannot meet them face to face.

As stated in the LSAG advisory note, ID&V methods may include using one or more of:

- Digital ID&V services meeting the requirements of the MLRs.[ii] See below: 'Choosing a Digital ID&V Service'.
- Using live and/or recorded video of the customer showing their face and original identification documents so that you can compare them to digital copies of the documents (i.e. scanned or photographed documents sent to you by email or post). You could use an app such as Zoom, WhatsApp, FaceTime or Skype.
- Collecting additional data to verify the information provided by the client, such as geolocation, IP addresses, or verifiable phone numbers etc.
- Verifying phone numbers and email or physical addresses by sending verification codes.

Choosing a Digital ID&V Service

The MLRs require that you satisfy yourself that a digital ID&V service is "secure from fraud and misuse" (R28(19)) and that it provides you with the appropriate level of assurance that your client is who they say they are. In deciding whether a service satisfies these requirements and whether you should use it, you should[iii]:

- Understand what it does and how it works. For example, which databases are checked?

- Take a risk-based approach to relying on the service based on the assurance level it provides.
- Understand whether different levels of assurance are available and how these should be used in different situations.
- Think about the effect using a particular service will have on the level of risk you attribute to non-face to face transactions.
- Use anti-fraud and other cyber-security measures to support the service.
- Consider whether the service has an accreditation or certification from any of the bodies in this list.
- Ensure the service provides you with the information you may need to provide to the CLC or law enforcement to show your compliance with the MLRs and keep records of this.

28 April 2020

[i] Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (MLRs).
[ii] A service must be "secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is the person with that identity", R28(19).
[iii] FATF (2020), *Guidance on Digital Identity,* pp.11-12.