Alternative Processes to Verify a Client's Identity

Guidance for Legal Practitioners

There are circumstances where it is not practical or possible for a client to meet with the legal practitioner face-to-face to verify a client's identity before accepting instructions. In addition, the COVID-19 pandemic has posed many challenges for legal practitioners, particularly during the period of social distancing, self-isolation and other disruptions to everyday business. This includes the difficulties associated with undertaking customer due diligence (**CDD**), including appropriate levels of identification and verification (**ID&V**), particularly where clients cannot be met face-to-face.

Meeting the ID&V obligations under Practice Direction P (PDP) and the Anti-Money Laundering Ordinance (**AMLO**) can be challenging in such circumstances, and can increase the risk of fraud, money laundering and terrorist financing. In such circumstances, legal practitioners can apply alternative methods of client identification. Legal practitioners are reminded to adopt a risk-based approach, taking into the account the circumstances of each individual client / matter.

As an alternative to face-to-face documentary verification, legal practitioners may adopt the following ID&V measures, where appropriate to the risks present in the client or transaction:

(1) use of an Agent;
(2) video conferencing method;
(3) dual verification process;
(4) third-party validation; and
(5) digital identity software.

1. Use of an Agent

Legal practitioners can accept certified copies of the client's identity documents, with the certification completed by an acceptable identity agent. An acceptable certified document is one that is certified by:

- a Notary Public;
- a Legal Practitioner;
- a Certified Public Accountant (practising);
- a Chartered Secretary;
- a Justice of Peace;
- a Consular or Embassy officer of the client's home country; or
- certification services.

Certification services that are recognized by the Electronic Transactions Ordinance (Cap. 553), such as the certification services available from the Hongkong Post or electronic certifications provided by certification authorities outside Hong Kong who have obtained mutual recognition

status from the Hong Kong Special Administrative Region Government, can be accepted for client identity verification purposes.

A list setting out the certificate types that have been granted mutual recognition status, method for verification of mutual recognition status and detailed verification information provided by recognised certification authorities are available at website of the Office of the Government Chief Information Officer of the HK SAR Government:

https://www.ogcio.gov.hk/en/our_work/business/mainland/cepa/mr_ecert/trust_list/hk_guangdong_ecert_trust.html

2. Video conferencing

Legal practitioners can use video conferencing tools (such as Skype, Zoom, FaceTime, WhatsApp or WeChat) to undertake verification of the client's identity documents. An identity verification process could include the following steps:

- Request that the client sends a clear image of their passport / ID document using a suitably secure means, for example an encrypted email;

- Arrange to video call the client. During this call, ask the client to hold the passport / ID document to their face. By checking the digital against the image of the client with the passport / ID document, the legal practitioner should be satisfied that they are one and the same person before proceeding;

- Capture screenshot of the client holding their passport / ID document to their face, you should date and attach a copy of that screenshot, as well as a copy of the client's passport / ID document initially provided, in the client file; or

- The legal practitioner can require a client to provide a clear, front-view 'selfie' of themselves that can be compared with the scanned or photographed copies of identification documents. This process should be supplemented by a call asking the client questions about their identification, their reason for requesting the service or other questions that would assist in ascertaining whether the client is who they claim to be.

3. Dual verification process

This process requires to review any two of the following pieces of information, each from a different reliable source who is not the client or an individual / entity acting on behalf of the client:

(1) Client's name and address;
(2) Client's name and date of birth;
(3) Client's name and confirmation that they have a deposit account, credit card, or other loan amount with a Financial Institution.

The legal practitioner must ensure that the information is provided by reliable sources for example:

Documents to verify name and address	Documents to verify name and date of birth	Documents to verify name and confirm a financial account
Document/Letter issued by the HK SAR Government	Birth Certificate	Mortgage document
Tax return	Marriage certificate or government-issued proof of marriage document (which includes date of birth)	Bank Statement
Immigration document	Divorce documentation	
	Driver's Licence	

As a mater of prudence, legal practitioners may ask the client to provide a 'selfie' picture of themselves which should be attached to client file.

4. Third-party validation

Legal practitioners can rely on certification undertaken by a professional known to the client for example a lawyer, doctor, an accountant, school principal, police officer. The professional is required to verify information that it holds on file for the client and e-mail both the client and the legal practitioner from its professional e-mail address. The e-mail or reference letter should include:

(1) their relationship with the client;
(2) how long they have known the client;
(3) their knowledge of the client's date of birth and address;
(4) that the photograph in the valid ID or passport document bears a true likeness to the client, their job title, full name, address and contact number.

For certifiers who are professionals, the legal professional should conduct an online check to establish the identity and profession of the certifier, their company / firm (if this is not obvious), and retain a screenshot of the same in the client's file.

In a higher risk situation, either do not chose this method of verification, or ask the referee to provide their own identity document before you provide any services.

5. Digital identity software

Law firms and practitioners are encouraged to use client identity verification software developed by third parties which undertake client checks remotely and securely. The service provider should be a reliable, independent digital ID system with appropriate built-in information security protocols which will help mitigate fraud risks. The benefits of the digital verification process have been highlighted by the Financial Action Task Force in their *Digital ID Guidance* published in March 2020, emphasising amongst other matters that non-face-to-

face onboarding and transactions conducted using trustworthy digital ID are not necessarily high-risk and can be classified as standard or even lower-risk.

All enquiries about this Guidance should be sent to the AML Executive at the Law Society on 2805 9101 or by email to aml@hklawsoc.org.hk