



How to verify your client

LIVE AML WEBINAR: 21 JUNE 2022

Today's presenters



Michelle Giddings,
Head of AML,
Professional
Standards
ICAEW



Sandy Price
AML Manager
Professional
Standards
ICAEW



Angela Foyle,
Head of Risk
Management and
Economic Crime
BDO Global



Vicky Soffa,
Director, Deputy
MLRO - Financial
Crime Team
Deloitte

Agenda

- Introduction
- Regulatory guidance
- Electronic verification
- Case studies
- Sources of verification
- Q&A



Polls

Please help us understand our audience
by answering our polls.

Money Laundering regulations s27 -30

Where the customer is beneficially owned by another person, the relevant person must

1. identify the beneficial owner;
2. **take reasonable measures to verify the identity of the beneficial owner so that the relevant person is satisfied that it knows who the beneficial owner is**

Beneficial Owner – Corporate entity (s5)

Any individual who exercises ultimate control over the management of the body corporate.

Any individual who ultimately owns or controls (in each case whether directly or indirectly), including through bearer share holdings or by other means, more than 25% of the shares or voting rights in the body corporate.

An individual who controls the body corporate.

Directors – who do I verify?

- CCAB AML Guidance for the Accountancy Sector– Appendix B
 - The names of directors should be verified on a risk-based approach.
 - The business should assess which directors require identity verification.
 - The subsequent work should include verifying both the director’s name and their identity – ie, that they are who they say they are.
 - For a normal risk client, the business should verify the identity of the director who is the key client contact.
 - Verification of additional directors should be considered for high-risk clients.

Beneficial owners of other types of entity

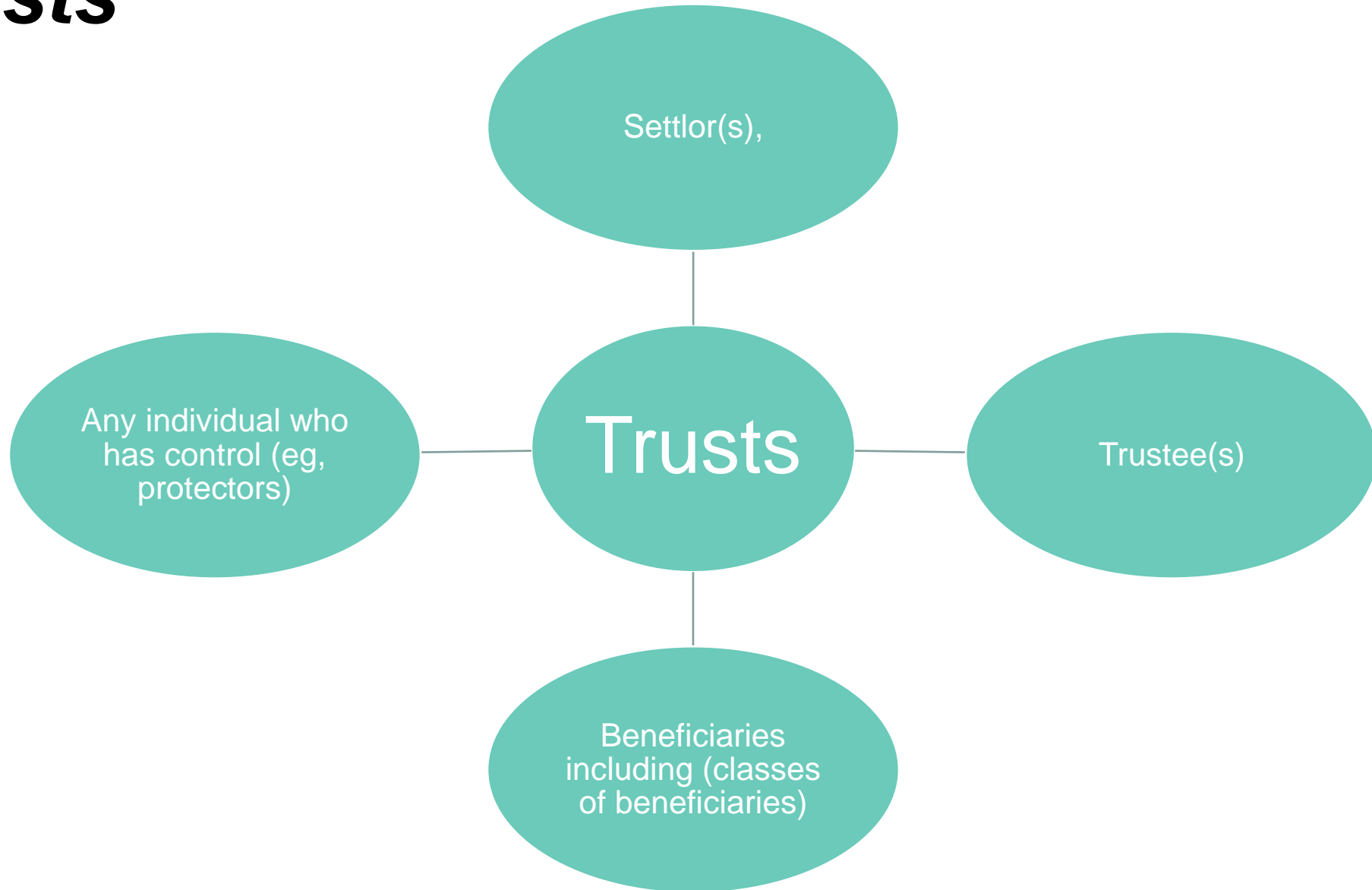
MLR17

- Regulations 5 and 6 define the meaning of 'beneficial owner' for a range of different client types.

CCAB AML GUIDANCE FOR THE ACCOUNTANCY SECTOR

- Paragraph 5.1.16
- Appendix E gives further examples

Trusts



Electronic verification

- Does the system draw on multiple sources?
- Are the sources checked and reviewed regularly?
- Are there control mechanisms to ensure data quality and reliability?
- Is the information accessible?
- Does the system provide adequate evidence that the client is who they claim to be?
- How are politically exposed persons (PEPs) defined?
- Are there searches of adverse media coverage?



Case studies

Case study 1: Facts

- Simon is the sole director of a newly established UK based company. He tells you that the holding company is a Maltese company and has two beneficial owners. Simon is one, he is a UK national, and the other is a friend, Alex, who has Maltese citizenship.
- The company will be involved in property management and rental.
- They plan to purchase a portfolio of properties. Property values will be in the millions.
- They want you to prepare and file statutory accounts and provide a registered office address for them. They would also like you to run the UK payroll, prepare and file statutory accounts
- Simon is going to set up a UK bank account but, in the meantime, can they use your client account to pay their staff? They will transfer the money from a bank account in Europe. They might need to make some payment to suppliers too so perhaps you could help with those transactions?

Case study 1: Risks and verification

Risks

- Malta is high risk jurisdiction
- Source of funds / wealth
- Use of client account
- Overseas links Russian sanctions regime
- Property

Verification

- Enhanced due diligence required
- Verification of the beneficial owners
- Public Register of Authentic identity and travel Documents Online (PRADO)
- Sources of wealth
- Sanctions checking
- PEP checks
- Open source checks – Google and adverse media checks
- Register of overseas entities

Case study 2: Facts

- A potential client asks the firm to provide tax services to both him personally and a company which he owns. The client has quite an uncommon name. As the work has been assessed as low risk for AML purposes and the client has been met and does not appear to have any higher risk factors associated with him, the firm decides to use electronic verification. Under the firm's procedures, a proportion of the onboarding files are sent to the MLRO for review as a quality check. This was one of those selected (before any engagement letter was signed).
- The MLRO notes that the electronic verification report highlights a risk factor – namely that an individual of the same (unusual) name and same address has been noted on the register of deaths.
- The MLRO telephones the partner to ask about this. The partner indicated that he had seen this but knew it must be an error because he had met the individual the previous week and he was alive and in perfect health. The MLRO raised the possibility that the client could be using a false identity.

Case study 2: Risks and verification

- The firm obtained a copy of the relevant death certificate and a saw the original of (and took a copy of) the passport of the prospective client as well as obtaining a copy of his birth certificate.
- On examination of these documents, it appeared that the deceased person was the father of the prospective client. The father had lived with his son and family in his final illness.

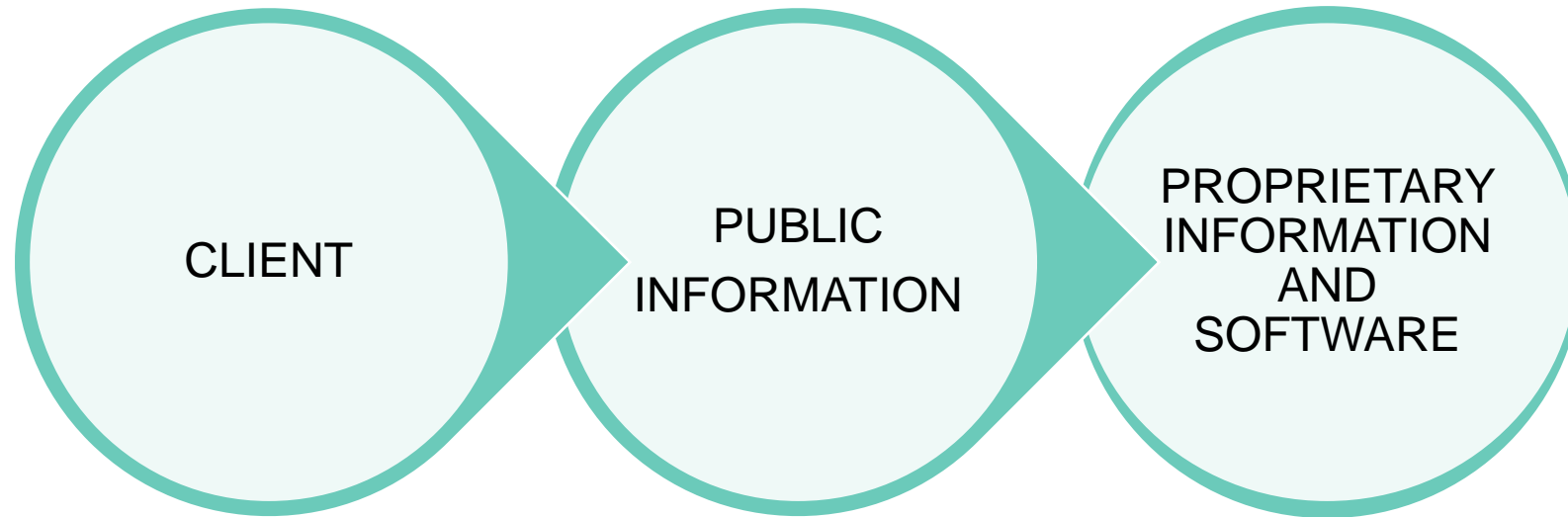
Case study 3: Facts

- A prospective client approached us to perform some tax work.
- The entity was 50% owned by Jim, and 50% owned by Nicola.
- Company's source of capital. Open-source searches on Jim showed he was a founder. For Nicola, there was nothing, including no mention of her on the company's own website.
- It is not unusual for a shareholder not to hold an active role in the client, however we still wanted to understand more on her source of wealth.
- Nicola was a nominee, holding the shares on behalf of her boss, Dave. Nicola was Dave's EA.
- Dave was the CEO of a retail group. There was a lot of information about Dave in the public domain.
- We understood the shareholdings, we obtained identity documents for Jim, Nicola and for Dave, we knew where the capital came from. Was there anything else we needed?

Case study 3: Risks and verification

- Taking a step back - why was there a nominee involved – if we don't know this, do we really understand the structure?
- Dave explained that he knew the founder, Jim, from university. The prospective client competes with a subsidiary in Dave's main businesses, so they didn't want the market to know they were backing a similar idea which might have raised questions over their conviction in that part of their own business.

Verification: sources



Verification: sources

- CLIENT SOURCED INFORMATION
 - Identity documents
 - Evidence of address
 - Trust documents
 - Power of Attorney
 - Probate documents
 - Other personal documents
- In many cases verification documents are held by the client.
- As noted in the CCAB AML Guidance for the Accountancy Sector, government issued documents (eg passports, driving licences) are a primary source of verification.
- For evidence of address, it is possible to use other sources (eg utility bills).
- Other documents may be obtained from the client but should be subject to further verification on a risk basis (eg confirming to public records or with a trusted professional such as a solicitor).

Verification: sources

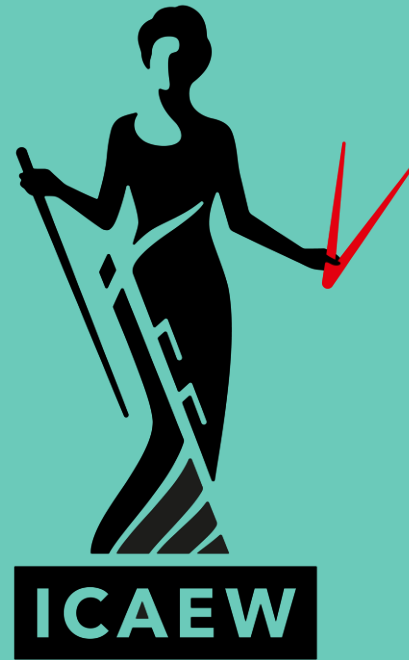
- PUBLIC SOURCES
 - Open source media (newspapers, civil society bodies, internet searches)
 - Companies House (but note that reliance may not be placed on this for beneficial ownership information)
 - Professional registers
 - Trade registers
 - Share registers
 - Other public registers or records (eg OFSI Consolidated List)
- Verification for low risk cases may be relatively straightforward, but in higher risk cases it may be necessary to seek further information to support the verification process.
- An example of this would be the verification of the type of business carried out by the client. There may be trade directories or professional registers which would support this.
- Open source media (including the Panama papers) can highlight areas of risk which may require further information or review before accepting the client.

Verification: sources

- PROPRIETARY SOURCES
 - Electronic sources of verification
 - Sanctions and politically exposed persons (PEP) screening software
 - Subscription services to fraud alerts
 - Subscription media services
 - Company data services
 - Credit reference agencies
- In addition to public sources of information and client personal documents, a variety of paid for services exist.
- These include electronic forms of identification. It is important to understand the sources against which the client data is checked and also the level of assurance provided. This is discussed further in the CCAB AML Guidance for the Accountancy Sector.
- With the increasing complexity of sanctions, for any practice with international clients, it is worth considering PEP and sanctions checking software.

Next webinar

- Our next webinar is on the topic of Cryptoassets.
- Date: 21 September | Time:12:00 – 13:30
- The panel will include ICAEW's AML supervision team, Nikhil Manek, MLRO for KPMG and representatives from BDO and the National Crime Agency.
- Look out for the registration link in the upcoming issue of AML, the essentials, on [LinkedIn](#), or at [icaew.com/events](https://www.icaew.com/events).



[icaew.com](https://www.icaew.com)