# COVID-19 anti-money laundering guidance for firms

As COVID-19 disrupts normal business activity, RICS understands that regulated firms may have concerns about how this impacts the processes and controls they have in place to comply with money laundering regulations, including requirements within the *Countering bribery and corruption, money laundering and terrorist financing* professional statement (February 2019).

The purpose of this document is to alert firms that they may face additional anti-money laundering (AML) and corruption risks at this time and identify some options available to maintain appropriate controls.

This document provides general advice for all regulated firms globally about compliance with the RICS professional statement. It does not provide legal advice on specific obligations for firms carrying out regulated activities. Firms may need to seek advice from a legal professional or contact their AML supervisor if they are concerned about compliance with legal obligations.

**Updating your anti-money laundering and bribery risk assessments**

The professional statement requires a risk-based approach to money laundering, terrorist financing, bribery and corruption, and firms have to evaluate the risks that both prospective and existing business relationships present.

These risk assessments should be reviewed in light of COVID-19 and the consequent changes to the business environment and the economy. In particular, firms should consider whether the current economic climate may make them or their customers more susceptible to financial difficulties or other pressures, thus creating risk and potential weaknesses for criminals to exploit.

Firms should be particularly alert to the following risks in new or prospective customers.

- Being asked to work with unusual customers on unfamiliar types of work.
- Resistance from potential customers to complying with due diligence checks, for example, being pressured to forego normal due diligence checks in order to speed up completion of the process.
- Becoming involved in work that is outside of the firm's normal area of experience and expertise without fully understanding the money laundering risks associated with that work.
- Transactions which do not have a clear business rationale or motivation.

Firms should continue to be alert to other money-laundering risks identified in their markets, for example in the UK, those set out in *Part 8 of HMRC's Estate agency guidance for money supervision* or in Hong Kong, Appendix B of the *Estate Agents' Authority Practice Circular 18-01*.

Firms should also be particularly careful about the risks of cybercrime as more communication with clients and within firms is done digitally. In particular it is important to be wary of intercepted emails (both internal and external) and criminals posing as solicitors. Changes to payment instructions should be verified using additional contact with clients via contact details held on file.

Also think about risks arising in the following four specific areas and whether the firm needs to put new or updated procedures and training into place.

## 1. Know your client procedures

The RICS professional statement requires firms to conduct appropriate checks to verify the identity of their clients and counterparties and, if necessary, identify their beneficial owners. Meeting the client in person is often part of this process and can provide assurance. However, in most cases this may not be possible or appropriate under COVID-19 restrictions.

It would therefore be reasonable for firms to put a specific COVID-19 process for identity checks in place, which may be reviewed as restrictions change.

The starting point is always to consider the risk profile of both the client and transaction. Based on the risk present in the transaction, firms must consider appropriate ways to carry out identity checks without face-to-face meetings. Customer identification and verification should not be relaxed due to COVID-19 restrictions.

The higher risk a transaction is, the more evidence the firm will need to collect to verify identity and the source of funds. The firm may need to consider not proceeding where the assessment indicates a high money laundering risk and appropriate verification cannot be achieved under current restrictions.

- **Using video streaming and scanned documents to identify clients.**

  One option, where it is allowed under any relevant national AML supervision guidance, is to use live video streaming services and scanned information to identify the client. At present, under HMRC guidance for estate agency businesses in the UK, this option is permitted for identification, but firms are required to verify the identity of the customer because of the risk that a forgery cannot be detected over a video conference. Verification will need to be achieved using either notarised copies, electronic verification or another format listed in Part 4 of the guidance.

  Where this option is permitted, the firm must ensure the security of both the scanned information – for example by using encryption – and the video streaming service. The UK Information Commissioner's Office and the UK, Canadian and Australian national cyber security centres have produced guidance on utilising video conferencing in a way that is safe and secure and ensures an adequate standard of data protection.

  The staff member carrying out identity checks on a video call should have a copy of the individual's identity documents. On the call the person should be asked to state their name, date of birth, first line of address, and to hold up their identity document so that it can be verified.

- **Using electronic identification tools.**

  Other options to carry out identity checks include using digital identification tools and verification can be provided through electronic services or notarised documents, as well as gathering and analysing other data to help to verify the person's identity. A combination of options may need to be used depending on the risk assessment.

  As always, firms must satisfy themselves that the method used and documentation provided is sufficient to verify the person's identity. The Financial Action Task Force (FATF) have recently published a *Guidance on Digital Identity* which firms may find helpful (*bit.ly/FATFgodi*).

- **Using third parties for client verification.**

  The RICS professional statement allows firms to rely on third parties (for example solicitors or estate agents acting for a counterparty), but only where there is an appropriate level of confidence in the quality of the information provided by the third party. The firm will need to check what processes the third party is employing and how they have been modified to take account of the current restrictions, because ultimate responsibility for the assessment of risk and actions taken based on this remain with the RICS professional or regulated firm. As noted above, you should also check what legislative requirements may apply to reliance provisions in your country.

### 2. Maintain thorough checks for existing clients

Although the identities of existing clients should already have been verified, it is important to recognise that money laundering activity could commence at any stage of a customer's relationship with a firm. Consequently, when receiving a new instruction from an existing customer, the firm should consider what they are being asked to do, the purpose of the work and whether that is consistent with their knowledge of the client or raises new money laundering risks. Information collected about existing clients should be kept up to date in line with the current risk assessment.

The firm should also periodically check identity information for existing clients and review this where a change is identified, and the same verification approach should be taken as for new clients.

### 3. Review staff responsibilities and training

The firm should consider whether they need any cover for staff who are or could fall ill, or who are on leave of absence who perform important functions in relation to money laundering, whether that is keeping records, auditing documents, or receiving internal reports of suspicious activities. If there are staff missing in the reporting line, you may need to train replacements to provide cover. Training can be delivered online.

The firm should communicate any changes to processes – for example in relation to identity checks – and any changes of responsibilities to all staff. It may also want to remind staff of their core AML duties and the procedures they need to follow

to counter AML and bribery and corruption. For many staff members there have been a lot of changes and increased pressures. It is therefore timely to provide a reminder about the importance of reporting suspicious activity, inducements or gifts, and that client pressure should not lead to shortcuts in due diligence procedures.

The obligation to report suspicious activity has not changed and staff should continue to report it to the nominated person in the firm, and they should continue to make appropriate reports to relevant authorities.

## 4. Review procedures and record keeping

If the firm's procedures are currently based on face-to-face meetings, or employee responsibilities have changed, the firm should amend written procedures to document this for all staff. Also make sure that colleagues working at home have access to digital copies of written procedures and any systems they need to record or report gifts, inducements or suspicious activities.

Firms have to record and retain information detailing how they have met the requirements of the RICS professional statement.

If you are using video conferencing to verify identities the firm will need to keep a recording of this. Firms should consider whether they need to obtain consent or update their privacy notice to cover this recording and provide participants with a short message and link to the privacy notice in the meeting invitation and on any registration page.

It is important to check whether any of the firm's AML record keeping is currently paper based and will need to be transferred to electronic records that can be accessed centrally while staff are working from home. The firm should also consider how to protect against documents being changed and maintaining an audit trail of any changes.