ISLE OF MAN
FINANCIAL SERVICES AUTHORITY
Lught-Reill Shirveishyn Argidoil Ellan Vannin

Anti-Money Laundering and Countering the Financing of Terrorism FAQs in relation to COVID-19

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

1. Introduction

The purpose of this document is to provide some guidance in relation to complying with the requirements of the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") whilst observing social distancing or self-isolation. The Authority are aware that the current situation is one that could be taken advantage of by criminals, and as such, there is a potentially heightened risk of money laundering at this time. It should be noted that although guidance is not law, it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa. This is a "living document" and will be added to as any further queries emerge.

2. FAQs

2.1 How to verify CDD documents whilst observing social distancing or self-isolation.

Relevant persons must verify the identity of customers, beneficial owners, and persons to whom loans or payments are being made in accordance with the requirements of the Code. The Authority recognises that COVID-19 may make it difficult for relevant persons to verify individuals using their normal processes. It remains vital to confirm that the customer is who they say they are and that the information or documents are checked/verified to ensure that they make sense and fit in with the customer's risk profile.

As per paragraphs 8(2) and 11(2) of the Code, CDD procedures and controls, including verification of identity, must be undertaken either before a business relationship is entered into, during the formation of that relationship; or before the occasional transaction is entered into.

There are a number of ways to verify information which has been provided whilst observing social distancing or self-isolation.

Information and documents will need to be considered at on a case by case basis in order to confirm if they assist in determining whether a customer is who they say they are. The relevant persons must also take into account the risk of both the customer and, if applicable, any introducer.

2.1.1 Meeting customers through video conferencing

Face to face contact for the verification of documents does not require parties to be physically in the same vicinity. Face to face contact includes the use of real-time visual communication media over the internet, such as full motion video conferencing. Scanned or photographs of documents can be received by the introducer, certifier or relevant person and can then be verified by a video call with the customer where they view both the documents and the customer. Where this option is used it must be documented for each case. If an introducer or suitable certifier has met the customer they must confirm to the relevant person that they have met the customer via video conferencing, including a photograph or scanned copy of the documents.

2.1.2 "Selfie" documents

As per section 12 of part 4[1] of the Anti-Money Laundering and Countering the Financing of Terrorism Handbook ("the Handbook") selfie verification is acceptable for identity documents, and the Authority considers that this is also acceptable for address documents. When using this form of verification a photograph should be provided which clearly shows the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy or photograph of the document itself should also be provided.

2.1.3 Statements and bills received in an e-format

As per section 8.1 of the Handbook, where statements of bills have been provided to the customer in an e-format they are acceptable provided that they clearly show the customer's residential address (not just an email address). These documents should then be verified via one of the methods outlined above in 2.1.1 and 2.1.2.

2.1.4 What to verify

Section 7 of the Handbook notes that in some cases a relevant person may be satisfied that a customer is who they say they are without needing to verify all suggested components of identity, for example; residential address of the customer. This is acceptable provided sign-off by senior management is obtained to ensure that the relevant person is satisfied that it's meeting its obligations under the Code[2].

2.1.5 Business Risk Assessments

The above measures may involve relevant persons deviating from their normal CDD practices and procedures, therefore the Business Risk Assessment should be updated to take into account variations that are taking place due to COVID-19.

[1] Please note part 4 of the AML/CFT Handbook has been revised and is currently in a separate stand-alone document. Any references to "Handbook" in this document are referring to the aforementioned stand-alone part 4 document.

[2] If a decision is made to implement a change for a class of customers this should be documented in the Business Risk Assessment. Once this has been documented it will no longer be necessary to obtain senior management sign of for every instance.

2.2 Staff training

Paragraph 32 of the Code mandates that relevant persons must provide education and training at least annually.

The Authority are aware that relevant persons may have training booked which has now been postponed/cancelled. In cases were training was postponed/cancelled due to COVID-19 and this means that the annual training deadline would be missed the Authority would take a pragmatic approach when assessing compliance with the Code. We would expect to see documentation that the person had organised or been booked on the course and that this had been cancelled due to the COVID-19. We would also expect to see that the relevant person had taken proactive measures to undertake some AML/CFT training before the course was rearranged (such as using online resources).

3. Signatures

The Authority expects regulated entities to consider whether a wet signature is required for legal efficacy or whether an electronic signature is acceptable legally and by the counterparty, and consider arrangements for witnessing such signatures where relevant.

The Electronic Transactions Act 2000 (ETA2000) will also be relevant in this regard.

Section 1 of the ETA2000 provides that a transaction will not be invalid merely because it takes place wholly or partly by means of one or more electronic communications.

The requirement for a written signature of a person is taken to have been met under the ETA2000 in relation to an electronic communication if:

1. a method is used to identify him and indicate his approval of that which is communicated;
2. having regard to all the relevant circumstances at the time, the method is as reliable as is appropriate for the purpose of the information communicated, and;
3. the receiver consents to that method.

Section 12 of the Handbook also allows client due diligence (CDD) documentation to be obtained electronically. The Handbook provides that where CDD is obtained electronically, the authenticity of the electronic document must be verified by appropriate measures.

If moving from wet signatures to electronic signatures, regulated entities should undertake and document a business and technological risk assessment.