E-ID as valid evidence of identity in Jersey

July 2019

The Jersey Financial Services Commission (**JFSC**) recently updated its AML/CFT Handbook for regulated financial services businesses (**Handbook**) to expressly permit evidence of identity to come from electronic sources (**E-ID**) as an alternative to original "wet ink" documents.

Background

The current version of the Handbook, which was first published on 1 January 2015, has been updated to reflect the Money Laundering (Amendment No. 10) (Jersey) Order 2019, which came into force on 12 June 2019.

The legislation was introduced in order to implement the 2012 FATF Recommendations on Anti-Money Laundering and Countering the Financing of Terrorism (**2012 FATF Recommendations**) in line with Jersey's policy of compliance with international AML/CFT standards and its commitment to the worldwide fight against financial crime.

E-ID as a source of evidence of identity

E-ID, which is described in the Handbook as "*the use of smart phone and tablet applications to capture information, copy documents and take photographs of customers as part of [a relevant person's] CDD processes*", is not expressly dealt with in the 2012 FATF Recommendations. However, the JFSC has recognised that developments in regulatory technology (**RegTech**) mean that, with the appropriate safeguards in place, E-ID could be an acceptable source of evidence of identity which complies with the requirements set out in the 2012 FATF Recommendations.

The changes to the Handbook include the addition of a reference to E-ID in the list of acceptable sources of evidence of identity at Section 4.3.2 of Part 1, alongside original "wet ink" documents, certified copy documents and external data sources.

The previous version of the Handbook already included guidance on the use of E-ID in customer due diligence (**CDD**) processes, which has been retained in the revised version. The guidance explains how legal and regulatory obligations in relation to CDD could be met using E-ID, taking into account the inherent risks associated with using new or developing technologies to obtain information (see below).

However, it was not previously clear whether E-ID was an acceptable substitute for "wet ink" identification documents, or whether it could only be used alongside more traditional forms of due diligence.

The revised Handbook provides welcome confirmation that E-ID can be used as an alternative source of evidence of identity, provided that the risks identified in the guidance have been considered and effectively managed.

Managing the risks – choosing the technology

The Handbook's guidance on the use of E-ID notes that smart phone and tablet applications ('apps') can be used to capture, transmit, compare and verify information, documents or photographs in CDD processes. Developments in RegTech and increased demand have seen the launch of a number of apps which can do some or all of these tasks, and the capabilities of these apps will only increase as the technology advances.

The guidance says that, when deciding whether to use a particular app, the user needs to consider certain inherent risks, including that documents or photographs could be tampered with or forged or that documents presented by a customer could have been stolen.

The guidance suggests various app features which may be used to mitigate the risks, such as comparing data on the identity document to biometric data, the automatic examination of data for the existence of security features such as watermarks and holograms, and the use of passwords and location matching.

Choosing the right app will therefore be an important decision – relevant persons intending to use E-ID in their CDD processes should research the different products on offer to assess their security features and should be prepared to invest accordingly.

Updates to policies and procedures

Weighing up the risks, making the decision to accept E-ID and choosing the right technology are only part of the picture – relevant persons also need to ensure their policies and procedures allow them to use E-ID.

Under the Money Laundering (Jersey) Order 2008 (as amended) (**Order**) a relevant person is required to establish and maintain "appropriate and consistent" policies and procedures relating to, amongst other things, its CDD measures in order to prevent and detect money laundering and financing of terrorism.

Specifically, Article 11(3)(bb) of the Order states that such policies and procedures must cover "*in relation to the use of new or developing technologies for new or existing products or services, the identification and assessment of associated risks before the launch of such technologies and the taking of appropriate measures to manage and mitigate those risks*".

Those polices and procedures must be documented in accordance with the Handbook.

It is therefore imperative that a relevant person's AML/CFT policies and procedures expressly allow it to use E-ID in its CDD processes (and specify the type of app or apps it has chosen to use) and that they identify the associated risks and set out measures for managing those risks.

Conclusion

Whilst the changes to the Handbook are to be welcomed, extreme care should always be taken when using E-ID to ensure that legal and regulatory obligations can be met, particularly where only E-ID is to be obtained to evidence identity, without any supporting original documentation.

A relevant person will need to demonstrate that it has fully considered the inherent risks in using the relevant technology and that it has taken appropriate steps to manage those risks. Policies and procedures should be reviewed before using E-ID and, in most cases, will need to be updated to cover the use of E-ID in CDD processes.