4 GUIDANCE ON PRODUCTS AND SERVICES

4.2 E-ID

4.2.1 Overview

1. The purpose of this section is to assist relevant persons who are considering the use of smart phone and tablet applications to capture information, copy documents and take photographs of customers as part of their CDD processes (referred to hereafter as "**E-ID**"). It:

   - explains the relevant legal and regulatory obligations in relation to CDD;
   - explains the relevant legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers;
   - highlights risk factors inherently associated with the use of smart phone and tablet applications to capture information, copy documents and take photographs; and
   - provides some examples of risk mitigants to consider when assessing use of a particular smart phone and tablet application.

2. This guidance may also be relevant in situations where similar processes, risks and potential mitigants are present (for example in assessing the risks presented by the use of self-service kiosks with similar document and image capturing and verification technology).

4.2.2 Background

3. In order to properly consider the risks associated with E-ID, it will be necessary for senior management to be very clear about what the smart phone and tablet application does and what it does not do. For example:

   - Is it to be used only to collect information about an individual from that individual?
   - Is it to be used to obtain evidence of that individual's identity?
   - Is it to be used to collect more general relationship information about an individual from that individual, e.g. source of funds?
   - Is it also to be used to collect information about an individual from reliable and independent data sources?

4. To the extent that a smart phone and tablet application does not cover particular elements of identification measures (or more general CDD measures), then, in line with Article 13 of the Money Laundering Order, these should continue to be applied using a relevant person's existing systems and controls (including policies and procedures).

4.2.3 Legal and regulatory obligations in relation to CDD

5. Article 3(4) of the Money Laundering Order explains that identification of a person means:

   - Finding out the identity of that person, including that person's name and legal status; and
   - Obtaining evidence on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who the person is said to be, and satisfies the person responsible for the identification of a person that the evidence does establish that fact.

6. Section 4.3.2 of the AML/CFT Handbook explains how a relevant person may demonstrate that it has obtained evidence that is reasonably capable of verifying that an individual to be identified is who the individual is said to be. Inter alia, it states that use of the following documentary evidence will be reasonably capable of verifying an individual's identity:

   - A current passport, or copy of such a passport certified by a suitable certifier;

- A current national identity card, or copy of such a national identity card certified by a suitable certifier; or
- A current driving licence, or copy of such a driving licence certified by a suitable certifier.

7. As an alternative to using documentary evidence, Section 4.3.4 of the AML/CFT Handbook permits, in certain circumstances, ***the use of independent data sources*** to verify that the person to be identified is who the person is said to be. In practice, it may be possible to demonstrate compliance with Article 3(4) of the Money Laundering Order through a combination of documentary evidence and independent data sources.

8. A relevant person may use other tools and/or methods (including E-ID) to undertake customer due diligence measures, so long as such methods comply with Article 3(4) of the Money Laundering Order.

4.2.4 Legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers

9. Article 11 of the Money Laundering Order requires a relevant person to have policies and procedures for the identification and assessment of risks that arise in relation to the use of new or developing technologies for new or existing products or services.

10. Article 15(3) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures when the customer has not been physically present for identification purposes.

11. An AML/CFT Code in Section 2.4.4 of the AML/CFT Handbook (and other Handbooks) requires a relevant person to assess, record and monitor risk when any element of the CDD process is outsourced to another party.

12. The Commission considers that all three requirements will apply in any circumstances where a part of the CDD process is undertaken by an independent third party via the use of new technologies where the customer is not present. Accordingly, when deciding whether to make use of a particular smart phone or tablet application, a relevant person is required to:

- Consider the risks involved in the use of the smart phone or tablet application and record the reasons why its use is appropriate.
- Consider the risks involved in outsourcing any part of the CDD process to an independent third party using the smart phone or tablet application and record the reasons why such outsourcing is appropriate.
- Consider whether the features of the smart phone or tablet application work to effectively mitigate the risks identified.
- Apply any additional measures to ensure that all risks are effectively managed.
- Apply on a risk-sensitive basis enhanced CDD measures to take account of the particular risks arising due to the fact that the customer has not been physically present for identification purposes.

13. For the avoidance of doubt, a risk assessment as described in this paragraph is not required to be undertaken on each occasion that the smart phone or tablet application is used, but rather when deciding whether to incorporate the use of the application into CDD measures.

4.2.5 Risks

14. The use of smart phone and tablet applications to apply identification measures presents a number of inherent risks. Typically, an application may do one or more of the following:

- capture information, copy documents and take a photograph of the customer (for instance by way of a camera on a smart phone or tablet);
- transmit the information, documents or photograph (either to the relevant person or another party);
- compare the information, documents and photograph captured;

- verify the information or documents against external data sources.

15. A relevant person may demonstrate that it has considered the particular risks that arise when using smart phone and tablet applications to copy documents and take photographs for CDD purposes when it considers the risks set out at sections 4.2.5.1 to 4.2.5.3.

4.2.5.1 The risk that identification documents are tampered with or forged

16. When original documents are not physically presented, it is more difficult for a relevant person to detect that documents have been tampered with or forged. For example, it may be difficult to detect that a photograph has been inserted into a passport, when simply viewing an electronic copy of the passport.

17. Similarly, it may be difficult to detect the presence or absence of watermarks or other security features on an identity document when simply viewing an electronic copy of the document.

4.2.5.2 The risk that captured copies of documents or photographs are tampered with before or during transmission

18. When an electronic copy of a document has been captured or photograph has been taken, there may be opportunities for the customer (or another party) to use software to alter the copy of the document or photograph before transmitting from the smart phone or tablet. For example, when a customer is merely transmitting a scanned copy of a passport, it may be possible to alter details (such as name, date of birth) on the copy of the passport prior to transmission.

19. Similarly, it may be possible to alter the biometric data (such as a photograph) on a copy of an identity document.

4.2.5.3 The risk that documents presented are stolen or their use unauthorised

20. When a customer is not physically presenting identification documents, it is more difficult for a relevant person to detect that the documents do not belong to the customer. For example, a customer may present stolen documentation.

4.2.6 Considerations for assessing applications

21. This section lists some potential features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risks listed at Section 4.2.5. Where the smart phone or tablet application (or connected system) does not sufficiently mitigate the risk, the relevant person will need to ensure that its CDD systems and controls include measures specifically designed to do so.

22. The list of features below is not exhaustive and other features or systems and controls may be appropriate.

4.2.6.1 Risk that identification documents are tampered with or forged

23. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that documents have been tampered with or forged may include:

- The copy of the document is of a very high level of clarity and resolution, such that its contents can be adequately viewed and/or enlarged to aid review;
- The copy of the document is automatically matched to a "template' for the particular form of identity document used;
- Data on the document is compared to biometric and other data stored on the machine readable code/algorithm on the document;
- Data on the document is automatically examined for use of unauthorised print fonts and unexpected character spacing;

- The copy of the document is automatically examined to confirm the existence of security features (e.g. watermarks, holograms, micro-text, etc.);
- The copy of the document is examined by individual(s) specifically trained to detect tampering/forgery (e.g. ex-border agents).

4.2.6.2 Risk that captured documents or photographs are tampered with before or during transmission

24. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that a copy of a document or photograph has been tampered with may include:

- The smart phone or tablet application itself controls the copying of the document, photography, and transmission process, allowing no opportunity to tamper with, or manipulate, documents or photographs. (Compared to, for instance, a prospective customer taking a photograph of a document and transmitting the pdf by e-mail);
- A highly secure connection is used to transmit copies of documents and photographs;
- Application security is regularly tested in order to guard against hacking or other security breaches.

4.2.6.3 Risk that documents presented are stolen or their use unauthorised

25. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that documents presented are stolen (or their use unauthorised) may include:

- A "selfie" photograph of the customer is taken and biometrically compared/matched to the photograph on the identity document presented - to verify that they relate to the same person;
- A video or "stream" of photographs is taken in order to identify facial movements - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised;
- A code or password is sent to the customer who, immediately before the application of E-ID, is photographed while displaying the code or password - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised;
- Use of a location match – where the application determines that information and copies of documents are captured and photographs taken at a location that is consistent with the customer's place (or country) of residence.

4.2.6.4 Record-keeping

26. Where a relevant person uses smart phone or tablet applications to capture information, copy documents and take photographs of customers as part of their CDD processes, adequate records must be kept in line with record-keeping requirements in Part 4 of the Money Laundering Order.