CONSULTATION PAPER NO. 9 2015

ELECTRONIC CDD

Consultation on proposals to provide additional guidance on the application of customer due diligence measures in the Handbooks for the Prevention and Detection of Money Laundering and the Financing of Terrorism for:

- Financial Services Business Regulated under the Regulatory Laws
- The Accountancy Sector
- The Legal Sector
- Estate Agents and High Value Dealers

ISSUED OCTOBER 2015

GLOSSARY OF TERMS

AML/CFT Handbook	means the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for Financial Services Business Regulated under the Regulatory Laws
CDD	means customer due diligence – as defined in Article 3 of the *Money Laundering Order*
Commission	means the Jersey Financial Services Commission
Commission Law	means the Financial Services Commission (Jersey) Law 1998
Four Handbooks	means the *AML/CFT Handbook*, *Handbook for the Accountancy Sector*, *Handbook for the Legal Sector* and *Handbook for Estate Agents and High Value Dealers*
Handbook for Estate Agents and High Value Dealers	means the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for Estate Agents and High Value Dealers
Handbook for the Accountancy Sector	means the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for the Accountancy Sector
Handbook for the Legal Sector	means the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for the Legal Sector
Jersey Finance	means Jersey Finance Limited
Money Laundering Order	means the Money Laundering (Jersey) Order 2008
Proceeds of Crime Law	means the Proceeds of Crime (Jersey) Law 1999
relevant person	means a person carrying on a financial services business (as described in Schedule 2 of the *Proceeds of Crime Law*) and which is carrying on that business in or from within Jersey, or, if a Jersey legal person, carrying on that business in any part of the world
Supervisory Bodies Law	means the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008

CONSULTATION PAPER

Changes are proposed to Section 4 of Part 4 of the *Four Handbooks.*

The *Commission* invites comments on this consultation paper. **William Byrne** at *Jersey Finance* is co-ordinating an Industry response that will incorporate any matters raised by its members. Comments should reach *Jersey Finance* by 20 November 2015.

Responses should be sent to:

William Byrne
Head of Technical
Jersey Finance Limited
4th Floor, Sir Walter Raleigh House,
48-50 Esplanade,
St Helier,
Jersey
JE2 3QB

Telephone: +44 (0) 1534 836000
Facsimile: +44 (0) 1534 836001
Email: william.byrne@jerseyfinance.je

Alternatively, responses may be sent directly to **Andrew Le Brun** at the *Commission* by 20 November 2015. If you require any assistance, clarification or wish to discuss any aspect of the proposal prior to formulating a response, it is of course appropriate to contact the *Commission*. The *Commission* contact is:

Andrew Le Brun
Director, Financial Crime Policy
Jersey Financial Services Commission
PO Box 267
14-18 Castle Street
St Helier
Jersey
JE4 8TP

Telephone: +44 (0) 1534 822065
Email: a.lebrun@jerseyfsc.org

It is the policy of the *Commission* to make the content of all responses available for public inspection unless specifically requested otherwise.

Contents

1 EXECUTIVE SUMMARY

1.1 Overview

1.1.1 This consultation paper seeks feedback on a proposal to add a new chapter to Section 4 of Part 4 of the *Four Handbooks.*

1.1.2 The amendments are proposed in order to recognise that technology now offers the possibility of collecting information about a customer who is an individual and obtaining evidence of that individual's identity in new and different ways.

1.1.3 While the use of technology is not inconsistent with *CDD* requirements and guidance currently provided, the *Commission* considers that additional guidance may be useful where wholly new concepts are adopted, such as the use of smart phone and tablet applications to apply identification measures.

1.2 What is proposed and why?

1.2.1 It is proposed to add a new chapter to Section 4 of Part 4 of the *Four Handbooks,* entitled "New technologies for applying CDD measures".

1.2.2 A draft of the proposed new chapter is attached as Appendix B.

1.3 Who would be affected?

1.3.1 The proposal to add a new chapter to Section 4 of Part 4 of the *Four Handbooks* will affect all *relevant persons* that are considering use of, or using, smart phone and tablet applications to apply *CDD* measures.

2 CONSULTATION

2.1 Basis for consultation

2.1.1 The *Commission* has issued this consultation paper in accordance with Article 8(3) of the *Commission Law*, as amended, under which the *Commission* "*may, in connection with the carrying out of its functions - ….consult and seek the advice of such persons or bodies whether inside or outside Jersey as it considers appropriate*".

2.2 Responding to the consultation

2.2.1 The *Commission* invites comments in writing from interested parties on the proposals included in this consultation paper. Where comments are made by an industry body or association, that body or association should also provide a summary of the type of individuals and/or institutions that it represents.

2.2.2 To assist in analysing responses to the consultation paper, respondents are asked to:

2.2.2.1 prioritise comments and to indicate their relative importance; and

2.2.2.2 respond as specifically as possible and, where they refer to costs, to quantify those costs.

2.3 Next steps

2.3.1 Following consultation, the *Commission* will give effect to appropriate changes to the *Four Handbooks*.

3 THE COMMISSION

3.1 Overview

3.1.1 The *Commission* is a statutory body corporate established under the *Commission Law*. It is responsible for the supervision and development of financial services provided in or from within Jersey.

3.2 Commission's functions

3.2.1 The *Commission Law* prescribes that the *Commission* shall be responsible for:

3.2.1.1 the supervision and development of financial services provided in or from within Jersey;

3.2.1.2 providing the States, any Minister or any other public body with reports, advice, assistance and information in relation to any matter connected with financial services;

3.2.1.3 preparing and submitting to the Minister recommendations for the introduction, amendment or replacement of legislation appertaining to financial services, companies and other forms of business structure;

3.2.1.4 such functions in relation to financial services or such incidental or ancillary matters –

- as are required or authorised by or under any enactment, or
- as the States may, by Regulations, transfer; and

3.2.1.5 such other functions as are conferred on the *Commission* by any other Law or enactment.

3.3 Guiding principles

3.3.1 The *Commission's* guiding principles require it to have particular regard to:

3.3.1.1 the reduction of risk to the public of financial loss due to dishonesty, incompetence, malpractice, or the financial unsoundness of persons carrying on the business of financial services in or from within Jersey;

3.3.1.2 the protection and enhancement of the reputation and integrity of Jersey in commercial and financial matters;

3.3.1.3 the best economic interests of Jersey; and

3.3.1.4 the need to counter financial crime in both Jersey and elsewhere.

3.4 Commission's role with respect to AML/CFT

3.4.1 With respect to the need to counter financial crime in both Jersey and elsewhere, the *Commission* is the supervisory body that exercises supervisory functions in respect of:

3.4.1.1 regulated persons[1]; and

3.4.1.2 persons carrying on a specified Schedule 2 business[1].

3.4.2 The supervisory functions to be exercised by the *Commission* are defined in Article 2 of the *Supervisory Bodies Law*, namely:

3.4.2.1 monitoring compliance by a supervised person[1] with, inter alia:

- any requirement to which that person is subject under the *Supervisory Bodies Law*;
- any Order made under Article 37 of the *Proceeds of Crime Law*;
- any direction under Article 6 of the Money Laundering and Weapons Development (Directions) (Jersey) Law 2012; and
- any Code of Practice that applies to that person or the supervised business[1] carried on by that person;

3.4.2.2 carrying out the functions, powers and duties conferred under the *Supervisory Bodies Law* for the purpose of compliance by a supervised person with the requirements described in 3.4.2.1.

3.4.3 In accordance with Article 22 of the *Supervisory Bodies Law*, the *Commission*, as the supervisory body, has prepared and issued a number of Codes of Practice. In each case, the Code of Practice comprises of a number of individual Codes of Practice which may be found in the *Four Handbooks*.

[1] These terms are defined in Article 1 of the *Supervisory Bodies Law*.

4 New technologies for applying CDD

4.1 Overview

4.1.1 This section proposes adding a new chapter to Section 4 of Part 4 of the *Four Handbooks*. The new chapter will provide guidance on the risks of using smart phone and tablet applications to capture copies of documents and take customer photographs as part of *CDD* measures.

4.1.2 It will also make it clear that the guidance on risks may be useful in other 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 Identification requirements in Jersey

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

4.2.1.1 finding out the identity of that person, including that person's name and legal status; and

4.2.1.2 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.

4.2.2 Section 4.3.2 of Part 1 of each of the *Four Handbooks* 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:

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

4.2.2.2 a current national identity card, or copy of such a national identity card certified by a suitable certifier; or

4.2.2.3 a current driving licence, or copy of such a driving licence certified by a suitable certifier.

4.2.3 As an alternative to using documentary evidence, Section 4.3.4 of Part 1 of each of the *Four Handbooks* allows 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.

4.2.4 Although there is currently no reference made to the use of smart phone and tablet applications in the *Four Handbooks*, there is nothing to preclude their use in *CDD* measures, so long as the *relevant person* complies with Article 3(4) of the *Money Laundering Order*.

4.3 Requirements that are relevant to the use of new technologies for applying CDD

4.3.1 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.

4.3.2 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.

4.3.3 An AML/CFT Code requires a *relevant person* to assess, record and monitor risk when any element of the *CDD* process is outsourced to another party.

4.3.4 The *Commission* considers that these requirements will apply in any circumstances where any part of the *CDD* process is applied by a third party via the use of new technologies where the customer is not present. The effect of this is that, when deciding whether to make use of a particular smart phone or tablet application, a *relevant person* is required to:

4.3.4.1 Consider the risks involved in the use of the smart phone or tablet application and record the reasons why its use is appropriate.

4.3.4.2 Consider the risks involved in outsourcing any part of the *CDD* process via the smart phone or tablet application and record the reasons why such outsourcing is appropriate.

4.3.4.3 Consider whether the features of the smart phone or tablet application work to effectively mitigate the risks identified.

4.3.4.4 Apply any additional measures to ensure that all risks are effectively managed.

4.3.4.5 Apply on a risk-sensitive basis enhanced *CDD* measures to take account of the particular risks that arise where a customer has not been physically present for identification purposes.

4.4 Risk assessment guidance

4.4.1 In order to assist *relevant persons* with the measures described at section 4.3.4 above, the *Commission* considers that it will be useful to provide guidance on the risks of using smart phone and tablet applications to capture copies of identification documents and to take photographs of customers.

4.4.2 The *Commission* considers that the particular risks that arise when using smart phone and tablet applications to capture copies and take photographs are:

4.4.2.1 the risk that identification documents have been tampered with or forged;

4.4.2.2 the risk that copies of documents or photographs are tampered with before or during transmission to the *relevant person*; and

4.4.2.3 the risk that documents presented are stolen or their use unauthorised.

4.4.3 The *Commission* also considers that it will be useful to provide guidance in relation to potential measures that might be incorporated into the features of a smart phone or tablet application to mitigate such risks.

4.5 Proposal

4.5.1 It is proposed to add a new chapter to Section 4 of Part 4 of the *Four Handbooks*, entitled "New technologies for applying CDD measures".

4.5.2 A draft of the proposed new chapter is attached as Appendix B.

5 COST BENEFIT ANALYSIS

5.1 Costs

5.1.1 It is not anticipated that there will be any costs to Industry or the *Commission* arising from the publication of this guidance.

5.2 Benefits

5.2.1 The publication of this guidance will help to remove any doubts about the feasibility and legality of using new technologies for applying *CDD* – where risk is properly managed.

5.2.2 It will also encourage *relevant persons* to consider taking advantage of technological developments in the field of *CDD*, which may be more cost effective and/or "customer friendly".

6 QUESTIONS

6.1 **Do you consider any guidance provided in the new chapter of Section 4 of Part 4 of the *Four Handbooks* to be unclear?**

If yes, please identify which guidance (by paragraph) and explain why:

_____
_____
_____

6.2 Are there additional areas where guidance could be provided in the new chapter of Section 4 of Part 4 of the *Four Handbooks*?

If yes, please explain:

_____
_____
_____

APPENDIX A

List of representative bodies who have been sent this consultation paper.

The consultation paper has been sent to all members of the *Commission's AML/CFT* Steering Group. Members are listed on the *Commission's* website under *AML/CFT* Steering Group.

In addition, copies of this paper have been sent to:

- Association of English Solicitors Practising in Jersey
- Association of Investment Companies
- Chartered Institute for Securities & Investment – Jersey branch
- Digital Jersey
- Institute of Directors – Jersey branch
- Jersey Association of Directors and Officers
- Jersey Association of Trust Companies
- Jersey Bankers' Association
- Jersey Chamber of Commerce and Industry Incorporated
- Jersey Compliance Officers Association
- Jersey Estate Agents Association
- Jersey Finance Limited
- Jersey Funds Association
- Jersey International Insurance Association
- Jersey Motor Traders Association
- Jersey Society of Chartered and Certified Accountants
- Law Society of Jersey
- Personal Finance Society – Jersey branch

APPENDIX B

Draft new chapter of Section 4 of Part 4 of the *Four Handbooks*

4 Guidance on Products and Services

4.7 E-CDD – 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 as "**E-CDD**"). 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).

4.8 BACKGROUND

3. In order to properly consider the risks associated with E-CDD, 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).

4.9 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 anticipates ***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-CDD) to undertake customer due diligence measures, so long as such methods comply with Article 3(4) of the Money Laundering Order.

4.10 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 a 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 via 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.

4.11 RISKS

13. 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 a third party);
- compare the information, documents and photograph captured;
- verify the information or documents against external data sources.

14. 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 4.11.1 to 4.11.3.

4.11.1 The risk that identification documents are tampered with or forged

- 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.
- 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.

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

- When an electronic copy of a document has been captured or photograph has been taken, there may be opportunities for the customer (or a third 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.
- Similarly, it may be possible to alter the biometric data (such as a photograph) on a copy of an identity document.

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

- 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.

4.12 CONSIDERATIONS FOR ASSESSING APPLICATIONS

15. 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 4.11. 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.

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

4.12.1 Risk that identification documents are tampered with or forged

17. 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).

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

18. 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.

4.12.3 Risk that documents presented are stolen or their use unauthorised

19. 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 is then 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.