Annex to the Financial Services Businesses Handbook

Using Technology in the Customer Due Diligence Process

A.1. Technology Risk Evaluation

1. A financial services business must, prior to deciding whether to utilise an electronic method or system in its due diligence process, have identified and assessed the risks arising from its use and documented these in a technology risk evaluation.

2. If a financial services business decides to proceed with the electronic method or system, the financial services business's Board must approve the technology risk evaluation and that approval must be documented.

3. The Board must regularly review the technology risk evaluation in conjunction with its responsibility for oversight of compliance as described under section 2.3 of the Handbook. The Board must record its confirmation that compliance with the Regulations and rules in the Handbook is maintained by its utilisation of the electronic method or system.

4. The technology risk evaluation applies only to the use of, or potential use of: digital signatures; electronic certification; and electronic verification.

5. The technology risk evaluation need only be updated when significant changes or upgrades to systems are implemented.

A.1.1. Technology Risk Evaluation Scope

6. The technology risk evaluation should include, as a minimum, an evaluation of the provider, the electronic method or system and its anticipated use, together with any identified risks associated with these areas.

7. It is not essential that the technology risk evaluation extend to a highly technical comprehensive report on the specifications and functionality. The objective of the technology risk evaluation is to evaluate the risks inherent in the use of an electronic method or system.

8. The use of electronic databases does not require compilation of, or inclusion in, a technology risk evaluation. In such cases financial services businesses should monitor performance as part of their oversight of compliance monitoring obligations under rule 28.

DRAFT

A.1.2. Areas to Consider when Evaluating an Electronic Method or System

9. The following points are guidelines and examples of points to consider when undertaking a technology risk evaluation. The guidelines are not exhaustive of every factor for consideration, neither are they proposed as a checklist. The guidelines propose a wide range of factors that could be considered in order to cater for the different types of electronic method or service a financial services business might contemplate using. It is acknowledged that in some instances financial services businesses may elect to use alternative or a limited number of the factors listed due to the type of electronic method or system being introduced.

A.1.2.1. Data

- What are the data sources used and the level of accessibility?
- Where is the data stored?
- What are the levels of user security and accessibility?
- What are the methods used to transfer data and documents?
- Are there adequate controls regarding the security of data?
- Who owns the data and documentation collected? If an outsourced provider retains the data and documentation then is there a contract or contingency plan to recover any data in the event of any changes occurring in the relationship with the provider?
- Is there an ability to select and change the data sources used?
- Does the result of the change maintain compliance with data protection legislation?
- Is it necessary to obtain customer consent in order to obtain, research or retain data?
- What are the security controls surrounding the system?
- What is the testing undertaken by a provider to ensure that their data sources are and continue to be accurate and reliable?

A.1.2.2. Controls

- Does the financial services business's existing fraud prevention policy and procedures need alignment or require amendment to accommodate process changes introduced through the technology?
- Does the financial services business's business continuity plan consider and cater for contingency plans for disruption of the electronic method or system?
- Whether there are mechanisms in place to maintain consistency with current and any future changes in international standards and requirements?

A.1.2.3. External Service or Product Providers

- If an external provider is used, is there knowledge and documentation of the system and transparency of the methodologies used by the provider?
- Is there a capability to cancel any arrangement with an external provider?
- Does the provider have a business continuity plan?
- Are there any vulnerabilities to the sustainability of a provider through other market competitors replicating or providing a lower cost alternative?
- Are there any patent controls to prevent copying and replacement?

DRAFT

A.1.2.4. Information Sources

- What source(s) of information are used to corroborate any information provided and are they acceptable to the financial services business?
- Is there an independent and reliable source to corroborate any information?
- Are a wide range of qualitative and informative sources accessed to corroborate data?
- Are the data sources able to link an individual to both current and previous circumstances, i.e. can the method or system access negative information sources, such as databases on identity fraud and deceased persons?
- How is information matched and corroborated and is this effective?
- What is the extent of the data held, i.e. how up to date is it?
- Is it possible to obtain the full range of identification data or is there an alternative process to acquire mandatory ID data not included within the identification documents?

A.1.2.5. Processes

- What is the assurance of security and authenticity of the method used to validate a customer's details?
- If photographs are taken of an individual and/or documents, how are they compared and checked to ensure authenticity?
- Is a single photograph taken, a series of photos or a video clip acquired?
- Are biometric comparisons used to validate facial features?
- For e-passports does the system read the biometric and other data stored on the embedded chip within the passport and compare it to the data on the passport and that provided by the individual?
- For systems that obtain an individual's photograph and make a comparison against other documents, does it provide a clear match or a percentage of assurance?
- What detection methods are used to provide for changes in identification photographs?
- What is the quality of the electronic record; are photographs clear, in colour and can all data be viewed or enlarged to add clarity?
- What methods are used to ensure that any documents are not altered or tampered?
- Are the documents subjected to independent scrutiny by personnel skilled in identifying potentially fraudulent documents?
- What testing is undertaken to ensure that the new technology method/system can detect fraudulent customers and documentation?

A.2. Maintaining the Effectiveness of Policies, Procedures & Controls

10. A financial services business must ensure that its AML/CFT policies and procedures contain a description which adequately explains how the electronic method or system operates and interacts with its wider AML/CFT controls.

11. The Handbook requires financial services businesses to ensure that there are appropriate and effective procedures and controls in place which provide for the Board to meet its obligation to review its compliance arrangements. Financial services businesses should ensure that procedures and controls accurately include instances where an electronic method or system has been implemented so as to correctly depict their processes.

12. The obligations to identify and verify an individual or a legal body or legal arrangement remain unchanged regardless of the electronic method or system used for CDD purposes.

A.3. Electronic Certification and Digital Signatures

A.3.1. An Introduction to Digital Signatures

13. Digital signatures are based on Public Key Infrastructure ("PKI") technology and guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents. A digital signature should not be capable of being copied, tampered with or altered. In addition, because digital signatures are based on standard PKI technology, they can be validated by anyone without the need for proprietary verification software.

14. A digital signature is a secure method of cryptographically binding an electronic identity to a specific document. A digital signature is a mathematical technique used to validate the authenticity and integrity of an electronic message or document and creates a unique 'hash' based upon the data contained within the document or message being signed.

15. The use of digital signatures provides financial services businesses with the ability to send and receive documentation in an electronic format negating the requirement for an original ink signature or 'wet signature'.

A.3.2. Digital Signatures vs. Electronic Signatures

16. The term electronic signature is often confused with digital signature. Digital signature refers to the security technology used in e-business and e-commerce applications, including electronic signatures. An electronic signature applied with digital signature security provides added assurance to the receiving party of the provenance, identity and status of an electronic document. Additionally, a digital signature acknowledges informed consent and approval by a signatory and ensures the non-repudiation of documents.

17. An electronic signature is any electronic means that indicates either that a person adopts the content of an electronic message, or more broadly that the person who claims to have written a message is the one who wrote it. An electronic signature can

be as basic as a typed name or a digitised handwritten signature applied to a document as an image using a stylus.

18. An electronic signature can further be defined as data in electronic form that is attached to or logically associated with other electronic data and that serves as a method of authentication. An electronic signature is an unsecure method of signing a document and is vulnerable to forgery, copying and tampering. Additionally, an electronic signature does not provide an assurance to the receiving party that the document has not been changed, or that the person signing is who they say they are and that they intended to sign the document.

A.3.3. Key Documents

19. The following legislation are key references in respect of this facility:

- The Electronic Transactions (Guernsey) Law, 2000 as amended.
- The Electronic Signatures Directive 1999/93/EC.
- With effect from 1 July 2016 a new regulatory framework (910/2014/EU) will replace the Directive on Electronic Signature (1999/93/EC).
- EU Regulation 910/2014.

A.3.4. Document Security of Digital Signatures

20. Although a digital signature produces a tamper evident seal, financial services businesses should ensure that their procedures provide for confirmation of the authenticity of a digital signature. The procedures should also include the measures to be taken in the event that checks do not confirm the integrity of a digitally signed document.

A.3.5. Digital Signatures Technology Risk Evaluation

21. Due to the security controls and authentication of the source document, an attached digital signature provides confidence that the received document is genuine and not tampered with in any manner.

22. If a financial services business decides to accept and/or use digital signature technology then they should conduct a technology risk evaluation of the system and its anticipated use. Guidelines for the completion of a technology risk evaluation are included in Section A.1.

23. The technology risk evaluation for the use of digital signatures need only be conducted to the extent that the Board of a financial services business is satisfied that the use of digital signatures continues to maintain compliance with existing policies, procedures and controls.

24. The technology risk evaluation should extend to confirming that the digital signatory ("the sender") has appropriate authorisation controls in place regarding who is allowed to use the facility. The sender should be aware that receipt of documents that have a digital signature attached would be considered as authentic and authorised.

DRAFT

A.4. Electronic Certification of Due Diligence Data which is in Paper Form

25. This section applies specifically to the electronic certification of paper documents and not identification data received through the use of an electronic verification method or system as described in section A.5. below.

26. If a financial services business uses an electronic method or system for certification purposes then the rules stated in section 4.5.2 of the Handbook regarding suitable certifiers apply.

27. A financial services business must not employ an electronic method or system which enables a natural person to self-certify their personal identification documents.

28. Where a financial services business accepts electronic certification it must only do so under a digital signature.

29. Should the certifier accept the documentation presented then using digital encryption software the certifier will apply a digital signature to an electronic copy of the physical document.

30. Financial services businesses should use a risk-based approach when deciding whether the certification is adequate and meets the criteria described in paragraph 102 of the Handbook. Best practice is that the certification will incorporate the following:

- confirmation that the certifier has met the individual in question;
- confirmation that the certifier has seen the original(s) of the document(s) being certified;
- the date the document was certified; and
- adequate details about the identity of the certifier in order that the receiving institution can satisfy itself that the certifier is a suitable person in the circumstances.

31. The objective of electronic certification is to confirm a document is a true copy of an original document and financial services businesses should use a risk-based approach to determine whether they are satisfied this has been achieved and if not further measures should be applied.

A.4.1. Risk Mitigation Measures

32. The use of electronic certification is an acceptable form of validating the legitimacy of identity documentation but the accepting financial services business must be satisfied with the veracity of the certification processes.

DRAFT

A.5. Electronic Verification - Using Technology to Verify Identity

A.5.1. Introduction

33. Electronic verification is the use of an electronic method or system to verify, in whole or in part, the identity of a customer by matching specified personal information against electronically captured physical documentation and/or independent electronic sources.

34. The demand to provide faster servicing is increasing the level of development in the use of technology. Systems currently exist that provide varying degrees of certainty regarding the capture of identification data and verification of that information related to individual customers and connected individuals. These systems range in scope from the electronic capture of identification data and documentation on a face-to-face basis through to the self-capture of uncertified documentation by a prospective customer using an interactive application on a tablet or mobile phone.

35. Rule 87 stipulates the minimum verification requirements. Electronic verification can be used to verify all or any combination of these mandatory verification requirements. Where an electronic verification system does not provide for compliance with all of these requirements then other alternative methods must be used in conjunction with the electronic verification system.

36. Electronic verification is a record kept in an electronic format that contains authenticated core identity information about an individual. Examples include obtaining a photograph or series of photographs of an individual via an application. Photographs are also collected of the identification document(s) and address verification document(s) of the individual. The photographs of the individual and the identity documents are then reviewed and corroborated.

37. The integrated controls inherent within electronic verification applications can provide an acceptable alternative measure to that of Rule 101 when firms are identifying and verifying non-resident customers. Examples of these controls include the reading of biometric information integrated within the microchip on many modern passports or validating the veracity of an official document with its issuing authority. Ultimately it is for the Board to assess the robustness of the verification controls within the application as part of its technology risk evaluation.

A.5.2. Verification of Identity of a Natural Person Using Electronic Verification

38. The fundamental obligation is to establish that any natural person, customer, beneficial owner, underlying principal, third party or third party associate (if applicable) is who they claim to be. Financial services businesses that verify identity through the use of electronic verification must confirm a person's existence on the basis of appropriate identification data that meets the criteria described in chapter 4, Customer Due Diligence, section 4.4.2 of the Handbook.

39. Electronic verification can help:

- identify if there is a person in existence with the personal details of your prospective or existing customer;

DRAFT

- identify if the address details and history of residency are consistent with details held on commercial databases;
- identify whether there are any criminal judgments against the individual or recorded at the individual's residence;
- identify politically exposed persons or those that are subject to sanctions; and
- mitigate identification fraud through confirmation that the identity relates to a living person.

A.5.3. Verification of Identity of Legal Bodies Using Electronic Verification

40. Electronic verification of the legal status of a legal body can be achieved by accessing online company registry databases or commercial databases that access the legal body's records.

41. It is not sufficient to rely solely upon confirmation of registration with a company registry. A financial services business should ensure that it acquires company details that comply with the stipulated legal body identification and verification criteria described in section 4.6.1.

42. Identification and verification are only two parts of the CDD obligations upon firms. A financial services business should also obtain information on the purpose, intended nature of the relationship, and consider whether the profile is consistent with the financial services business's knowledge of the customer in accordance with the rules in Chapter 3 of the Handbook.

A.5.4. Electronic Verification Risk Mitigation Measures

43. Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and documentation on a customer, financial services businesses should be mindful of any additional risks posed by placing sole reliance on an electronic method or system. An example is that electronic verification can be impaired due to an inability to verify all of the required identification data.

44. Knowledge and understanding of the functionality and capabilities of the system can help provide assurance of its suitability. In particular, there should be certainty of the methods applied to match identification data. The use of more than one confirmation source to match data enhances the assurance of authenticity.

A.5.5. Sources Used to Corroborate Information

45. It is imperative that when a financial services business is determining the means to corroborate information, that the electronic method or system uses sources that are reliable and can sufficiently mitigate exposure to fraud.

46. When considering an electronic method or system financial services businesses should evaluate whether the data collected electronically has been entirely corroborated. For example if an identification document is photographed via an application, what checking occurs to validate the authenticity?

47. If the collected data is checked / compared against external data sources then the technology risk evaluation should include assurance that those external sources are

reliable. For example does the external data provider validate its data from an original source i.e. the identification document issuer?

48. To mitigate the risk of impersonation fraud, financial services businesses could add additional verification through the confirmation of details via a second commercial database or alternatively a further primary verification source. Commercial databases are those usually maintained by an entity that has access to current data collated from a reputable source e.g. address from national telephone records or electoral register. It is for the financial services business to determine choice of a database.

A.6. Record Keeping Requirements

49. The record keeping requirements detailed in chapter 12 of the Handbook remain unchanged. The use of technology to collect and/or store data and documents does not alter the obligations and requirements described in the Handbooks.

50. Financial services businesses should cover in their use of technology risk evaluation the retention of documents in electronic format to ensure they do not incur legal evidential difficulties, for example in civil court proceedings. Retention may be:

- by way of original documents;
- on microfiche;
- in a scanned form;
- in a computer or electronic form.

DRAFT