Guernsey Financial Services Commission

Consultation on Proposals to Enable Using Technology for Due Diligence Purposes

Issued 29 May 2015

Guernsey Financial Services Commission

The Guernsey Financial Services Commission invites comments on this consultation paper, preferably by e-mail by no later than 31 July 2015

Responses should be sent to:
Financial Crime Supervision & Policy Division
Guernsey Financial Services Commission
PO Box 128
Glategny Court
Glategny Esplanade
St Peter Port
Guernsey
GY1 3HQ

Telephone: +44 (0) 1481 712706
Email: AMLCFT@gfsc.gg

If you require assistance or clarification in respect of any aspect of the proposals prior to formulating a response, the Commission contacts are:

Steve Chandler, Policy Advisor – Financial Crime Supervision & Policy Division.

Fiona Crocker, Director - Financial Crime Supervision & Policy Division.

CONTENTS

Glossary of Terms

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism.
CDD	Customer Due Diligence.
Digital signature	A secure method of cryptographically binding an electronic identity to a specific document.
Electronic method or systems	Digital signatures, electronic certification and electronic verification.
Electronic Signature or E-signature	Electronic equivalent of a written signature.
Electronic certification	The process by which customer due diligence documentation is validated by a suitable third party using electronic methods of certification.
Electronic verification	Use of electronic systems 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.
GFSC	Guernsey Financial Services Commission.
Handbooks	The Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing. The Handbook for Legal Professionals, Accountants and Estate Agents on Countering Financial Crime and Terrorist Financing.

1. Introduction

1. This consultation paper seeks feedback from the financial services industry on a number of proposals to amend the Bailiwick's Handbooks for financial services businesses and prescribed businesses on countering financial crime and terrorist financing.

2. It is an invitation to industry to work with the Commission to endeavor to ensure that the Bailiwick AML/CFT regime provides for the use of advances in technology in fulfilling their due diligence obligations.

3. The consultation runs until 31 July 2015.

4. The Commission invites comments from interested parties on the questions and proposals included in this consultation paper.

Any questions can be emailed to Steve Chandler, Financial Crime Supervision & Policy Division. AMLCFT@gfsc.gg

1.1. Why We Are Consulting

5. The Commission is issuing this consultation paper on proposed changes to the rules and guidance in the Handbooks on Countering Financial Crime and Terrorist Financing for Financial Services Businesses and Legal Professional, Accountants and Estate Agents (together "the Handbooks") following representation from industry that the present AML/CFT framework hinders firms from taking advantage of technological developments in the field of customer due diligence ("CDD").

6. The Commission recognises that technology is changing traditional methods of undertaking due diligence. Demand from industry for alternative cost effective and customer friendly options is resulting in the development and implementation of a variety of alternative technical options that capture and deliver due diligence components through the internet, tablets or smartphone applications. At the same time the Commission must ensure that appropriate regulatory safeguards remain in place requiring firms to maintain robust AML/CFT controls, of which an appropriate technological service or product can form part. It is therefore proposing rules that:

   - Firms must assess and document the risks of using a technological product or service as part of their AML/CFT controls and confirm that compliance with regulatory obligations will be met.
   - Firms' compliance monitoring arrangements must include periodic assessment that the technological product or service remains suitable for their business.

7. The Commission will be introducing an annual Financial Crime return. As part of the data collected in that, a firm will be required to state whether it is using any electronic products or services as part of its AML/CFT controls.

8. The Commission is also proposing amendments to a number of rules in the Handbook to provide firms with clarity over the use of an appropriate technological product or service within their AML/CFT framework.

1.2. The Timeframe for Change

9. The Commission is proposing to issue amendments to the current Handbooks upon conclusion of the evaluation of the consultation results.

10. The Commission had intended to include guidance on the use of technology within its wider exercise to revise the Handbooks, which commenced last year. However that exercise, whose principal objective is to bring both Handbooks up to FATF 2012 Recommendation standards has been pushed back as the schedule for the consideration of MONEYVAL mutual evaluation report of the Bailiwick of Guernsey has been changed from April to September 2015.

11. As there is a wider ongoing project to revise the Handbooks it is intended to incorporate the changes made as a result of this consultation into that revision in due course.

1.3. How to Respond

12. The consultation period runs from 29 May 2015 to 3pm, 31 July 2015. Participants are encouraged to feed back any comments as soon as possible. Responses are invited from all interested parties.

1.4. Completion of the Consultation Period

13. Upon completion of the consultation period the Commission will:

- Consolidate the replies received;
- Review the submissions;
- Amend the proposals as appropriate;
- Issue a summary of the feedback received; and
- Consolidate the rules and guidance into the current FSB & PB Handbooks and publish interim updated versions.

2. Structure of the Consultation Paper

14. This paper, which includes a synopsis of the technological products and services available, is structured to show the changes that are proposed to the existing chapters in the Handbooks regarding corporate governance, a risk based approach, customer due diligence and record-keeping. References are made to the relevant regulations in the Criminal Justice (Proceeds of Crime) (Financial Services Business) (Bailiwick of Guernsey) Regulations 2007 and/or the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008. Power to amend these regulations rests with the States of Guernsey Policy Council.

15. The Commission has determined that there is no need to propose to the Policy Council any changes to these regulations to accommodate the use of appropriate technological products and services into the Handbooks. However the Commission is reproducing the relevant regulations to show how the regulatory framework encompasses the use of appropriate technological products and services.

16. This consultation addresses three types of technological products and services:

- Digital signatures
- Electronic certification
- Electronic verification

Where relevant these three areas are collectively referred to as "Electronic Methods or Systems".

3. Next Steps

17. The Commission will take all responses to its' consultation into account when it finalises the changes to be made to the rules and guidance in the Handbook.

4. Digital Signatures.

Consultation

In order to enable firms the option to use digital signatures the Commission is proposing to include a description of the compliance measures to be implemented prior to use.

New or Amended Rules & Guidance

The Commission is proposing to add a new section, as shown below, after the rules and guidance in the FSB and PB Handbooks, Section 4.2 Customer Due Diligence – Policies, Procedures and Controls.

Within the digital signature section the Commission proposes to add three new rules. The first rule is to ensure that firms have procedures in relation to authenticating receipt of a digitally signed document.

The second rule and third rule are to make senders and recipients aware of the reliance placed upon the authenticity of a document signed with a digital signature. To prevent misuse, the rules requires firm to seek assurance that the sender has adequate security and controls surrounding use and that it is not possible for an unauthorised person to apply a digital signature.

New Rules

The proposed new rules in this section are shown in the grey highlighted boxes at points 11, 14 & 15.

4.1. Digital Signatures

1. 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.

2. 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.

3. The use of digital signatures provides firms with the ability to send and receive documentation in an electronic format negating the requirement for an original ink signature, (a.k.a 'wet signature').

4.2. Electronic Signatures

4. 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.

5. 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.

4.3. Electronic Signatures - Key Legislation

6. The Electronic Transactions (Guernsey) Law, 2000 as amended.

7. The Electronic Signatures Directive 1999/93/EC.

8. EU Regulation 910/2014.

4.4. E-Signature

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

4.5. Document Security

10. A digital signature produces a tamper evident seal.

11. A firm must ensure that their procedures provide for confirmation of the authenticity of a digital signature. The procedures must also include the measures to be taken in the event that checks do not confirm the integrity of a digitally signed document.

4.6. Digital Signatures Risk Assessment

12. 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.

13. If a firm decides to accept and/or use digital signatures then the business should conduct a technology risk evaluation of the system and anticipated use.

4.7. Authorisation of Digital Signature Users

14. A firm must ensure that as part of its arrangement to use digital signatures the sender has procedures in place for control and use. The controls the sender has in place must include who may apply a digital signature.

15. A firm must ensure that any sender of a digital signature is aware of the reliance placed upon the digital signature and that the firm will be considering as equivalent to an authorised ink signature.

5. Electronic Verification

Consultation

The Handbooks do not currently prevent firms using electronic verification. Guidance points FSB Handbook 88 & 89 & PB Handbook 102 & 103 include examples of documents that can be used for identification purposes and confirmation that the listed examples are not the only possibilities available.

New or Amended Rules & Guidance

The Commission is proposing to add a new section, as shown below, after the rules and guidance in the FSB and PB Handbooks, Section 4.4.2 Verification of Identity – the individual.

New Rules

The proposed new rule in this section is shown in the grey highlighted box, point 13.

5.1. Electronic Verification - Introduction

1. Electronic verification is the use of electronic systems 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.

2. 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 and verification of customers and connected parties. 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.

3. Electronic verification is a record kept in an electronic format that contains authenticated core identity information about an individual. E-verification is using the electronic record to verify a person's identity during the due diligence process.

4. Examples are obtaining a photograph or series of photos via an application. Photographs are also collected of the identification document and address verification document. The photographs are then independently reviewed and corroborated.

5.2. Electronic Verification Risk Mitigation Measures

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

6. 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.

5.3. Sources Used to Corroborate Information

7. The following are examples of the primary sources an electronic method or system could use to corroborate or obtain information:

   - passport issuing office;
   - driving licence issuing authority;
   - company registries;
   - electoral roll; and
   - commercial or electronic databases.

The above list is not an exhaustive list of all the available sources.

8. It is imperative that when a firm is determining the means to corroborate any information that the sources used are reliable and can sufficiently mitigate exposure to fraud.

9. When considering an electronic method or system firms should ascertain 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?

10. If the collected data is checked / compared against external data sources then the risk analysis should include assurance that those external sources are reliable. For example does the external data provider validate their data from an original source i.e. the identification document issuer?

11. To mitigate the risk of impersonation fraud, firms could add additional verification through the confirmation of details via a second commercial database.

5.4. Verification of Identity of a Natural Person Using Electronic Verification

12. 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. Firms 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 the CDD section of the Handbooks.

13. FSB Rule 87 and PB Rule 101 stipulate the minimum verification requirements. Electronic verification can be used to verify all or any combination of these mandatory verification requirements. Where electronic verification does not complete all these requirements then other alternative methods must be used by the firm to meet FSB Rule 87 and PB Rule 101.

14. Electronic verification can help:

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

5.5. Verification of Identity of Legal Bodies Using Electronic Verification

15. 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.

16. It is not sufficient to rely solely upon confirmation of registration with a company registry. A firm must ensure that it acquires company records that comply with the stipulated legal body identification and verification criteria described in the Handbooks, FSB & PB section 4.6.1.

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

6. Electronic Certification

Consultation

The Commission is proposing to add a new section, as shown below, after the rules and guidance in the FSB and PB Handbooks, Section 4.3 Obligation to Identify Customer Due Diligence – Policies, Procedures and Controls.

New or Amended Rules & Guidance

The Handbooks do not currently prevent firms using electronic certification, however the current rules and guidance do not provide specific instruction on the implementation and continuing use of an electronic certification method or system. The Commission is proposing to add the following rules and guidance to the current section.

Section 4.5.2 Suitable Certifier

The Commission is proposing adding an additional rule and guidance, as shown below, after the existing FSB Handbook Rule 106 & PB Handbook Rule 120.

The Commission is proposing that electronic certification can only be used where there is additional security added by a digital signature on the document.

New Rules

The proposed new rules in this section are shown in the grey highlighted boxes at points 5, 6, 7, 8, 9, 10, and 11.

6.1. Electronic Certification - Introduction

1. Electronic certification is the process by which customer due diligence documentation is validated by a suitable third party using electronic methods of certification.

2. Electronic certification requires the customer to present themselves, together with their physical documentation verifying aspects of their identity, to a suitable, independent third party individual, for the purpose of the third party validating that they have both seen the documentation verifying identity and secondly that the customer is the person depicted within the documentation provided.

6.2. Electronic Certification - Process

3. 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.

4. The certification will incorporate:

   - confirmation that they have met the individual in question;
   - confirmation that they have 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.

5. The rules stated in the Handbooks regarding suitable certifiers apply to electronic certification; in particular, a suitable certifier must certify that they have seen the original documentation.

6. A firm must not employ a method or system which enables a natural person to self-certify their personal identification documents.

7. Where a firm accepts electronic certification it must only do so under a digital signature.

8. A customer submitting their data and documents themselves via a portal, phone or tablet qualifies as data collection. Independent verification must be undertaken to authenticate the details.

6.3. Electronic Certification Risk Mitigation Measures

9. The use of electronic certification is an acceptable form of validating the legitimacy of identity documentation provided the accepting firm are satisfied on the following points:

10. Firms must be aware that the reliance upon alternative methods of certification is a matter for their assessment based upon their understanding of the veracity of the certification processes.

11. Firms utilising systems for electronic certification must be satisfied that there are adequate controls built in to the system to appropriately validate the authenticity of the identity documentation.

7. Implementing Technology for Due Diligence Purposes.

Consultation

Responsibility for compliance with the Regulations and rules in the Handbooks rests with the board of a financial services business or prescribed business. A Board is responsible for establishing and maintaining effective compliance monitoring programmes which are relevant to its business. It is therefore important that a FSB/PB utilising electronic methods and systems ensure that it continues to remain relevant for its business as the products and services it offers might change and the profile of its customer base alter over time.

Consequently prior to a Board, or senior management equivalent forum where the firm is a branch or subsidiary, taking a decision to implement an electronic system or method into its due diligence process the firm should assess the technological and outsourcing risks posed. Therefore, the Commission proposes making mandatory a requirement for a technological risk assessment to be undertaken and documented.

In order to ensure that an electronic method or system remains appropriate the FSB/PB must know and understand how it works. The Commission is therefore proposing to make mandatory periodic reviews to ensure that the electronic method or system remains appropriate and the FSB/PB holds information on how it works.

New or Amended Rules & Guidance

Section 2.3 Board Responsibility for Oversight of Compliance

The Commission is proposing the following amendments to existing FSB Handbook Rule 28 & PB Handbook Rule 44 as shown below:

A FSB/PB must also ensure that there are appropriate and effective policies, procedures and controls in place which provide for the Board to meet its obligations relating to compliance review. In particular the Board must:

- ensure that the compliance review policy takes into account the size, nature and complexity of the business and includes a requirement for sample testing of the effectiveness and adequacy of the policies, procedures and controls, including where aspects of the due diligence process are undertaken via electronic methods and systems;

Section 3.4 Business Risk Assessment – Management and Mitigation

The Commission is proposing adding the guidance shown below.

Amended Rule

The Commission is proposing an amendment to FSB Handbook Rule 71 & PB Handbook Rule 85 as shown below:

The FSB/PB compliance review policy must make provision for a review of the following elements to ensure their appropriateness and effectiveness:

- the procedures surrounding the products/services offered by the FSB/PB;
- the CDD requirements in place including the use of any electronic methods or systems for establishing a new business relationship or undertaking an occasional transaction;
- staff screening and training; and
- monitoring compliance arrangements.

New Rules

The proposed new rules in this section are shown in the grey highlighted boxes at points 3, 4, and 10.

7.1. The Application of a Risk Based Approach to Technology for CDD Purposes

1. Regulation 15 for both financial services businesses ("FSB") and prescribed businesses ("PB") makes provision in relation to the review of compliance. Regulation 15 for FSBs and PBs includes the following: *(Please note that for ease of reference the copy below is a combination of the FSB and PB Regulation).*

(1) A <*FSB/PB*> must-

(a) carry out and document a suitable and sufficient money laundering and terrorist financing business risk assessment which is specific to the <*FSB/PB*> -

(i) as soon as reasonably practicable after these Regulations come into force,

or

(ii) in the case of a <*FSB/PB*> which only becomes such on or after the date these Regulations come into force, as soon as reasonably practicable after it becomes such a business, and

(b) regularly review its business risk assessment, at a minimum annually, so as to keep it up to date and, where as a result of that review, changes to the business risk assessment are required, it must make those changes.

(c) ensure that a review of its compliance with these Regulations is discussed and minuted at a meeting of the board at appropriate intervals, and in considering what is appropriate a <*FSB/PB*> must have regard to the risk taking into account –

(i) the size, nature and complexity of the <*FSB/PB*>

(ii) it customers (*clients*), products and services, and

(iii) the ways in which it provides those products and services.

2. A firm should ensure, prior to adopting a specific electronic system or method, that they are satisfied that data capture and data validation will deliver the full extent of identity information and documentation required to comply with the applicable CDD requirements of the Regulations and rules in the Handbook.

3. A firm must ensure that its AML/CFT policies and procedures contain a description which adequately explains how the electronic method or system it utilises operates and complies with a firm's CDD obligations.

7.2. Technology Risk Evaluation

4. A firm must, prior to utilising an electronic method or system in its due diligence process, have identified and assessed the risks arising from the use of that service or product in advance of deciding whether to proceed. If a firm decides to proceed with the electronic method or system, the firm's Board must approve the technical evaluation and that approval must be documented. Such a technology risk evaluation must be documented in advance of implementation and retained for the minimum retention period.

5. If it is decided to use electronic methods or systems then a firm must conduct a technology risk evaluation of the provider, the system and its anticipated use.

6. The technology risk evaluation is not part of a business risk assessment; however reference to the risk evaluation should be included in the business risk assessment. The technology risk evaluation should be updated when changes or upgrades to systems are implemented. The references in the business risk assessment should also be updated as appropriate.

7.3. Maintaining the Effectiveness of Policies, Procedures & Controls

7. In assessing the suitability of an electronic method or system firms should consider whether the particular product/system delivers corroborated and verified information equal to, or exceeds, currently utilised methods.

8. The Handbooks require firms to ensure that there are appropriate and effective procedures and controls in place which provide for the Board to meet its obligations relating to their compliance review obligations. The assurance and reliance review is a component of FSB Handbook Rule 28 and PB Handbook Rule 44 through the obligation to test the effectiveness and adequacy of the policies, procedures and controls.

7.4. Obligation to Identify and Verify Using Electronic Verification

9. The obligations to identify and verify an individual or a legal body as described in the Handbooks remain unchanged regardless of the electronic method or system used for CDD purposes.

10. The Board must review the technology risk evaluation annually in conjunction with the effectiveness results of the sample testing. The Board must confirm as part of this review if compliance with the Regulations and rules in the Handbook is met by its utilisation of the electronic method or system results required under FSB rule 28 & PB Rule 44, as amended.

11. When considering an electronic method or system firms should evaluate the functionality and output against the basic CDD principles:

    - Obtaining information and data from and about the customer,
    - Identifying the customer (individual and legal entity) and, where the customer is a legal person or legal arrangement, the customer's ultimate beneficial owner;

- Verifying the customer's identity, and that of its beneficial owner where the customer is a legal person or legal arrangement, on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; and
- Understanding the purpose and intended nature of the relationship or occasional transaction and in higher risk situations, obtaining further information as required under the Handbook.

7.5. Areas to Consider when Assessing an Electronic Method or System

12. The following are examples of points to consider when undertaking an evaluation of technology in respect of an electronic method or system:

Data

- What are the range of 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?

Controls

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

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?

7.6. Compiling a Qualitative Assessment of an Electronic Method or System

13. When selecting or developing an electronic method or system firms should carefully consider the specifications, functionality and system architecture to confirm its viability and reliability. The following are examples of factors for consideration when selecting or developing a system or method. The list below is not an exhaustive list of factors and there may be others to consider:

Information Sources

- What source(s) of information are used to corroborate any information provided and are they acceptable to the firm?
- 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 it 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?

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 provided by the individual?
- For systems that obtain an individual's photograph and makes 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?

8. Record-Keeping, Electronic Data & Documents

Consultation

The Commission is proposing to add the following rules and guidance to the current section, after the rules and guidance in the FSB Handbook, Section 12 and PB Handbook, Section 10, Record-Keeping.

New or Amended Rules & Guidance

The Commission is proposing adding an additional rule and guidance, as shown below, after the existing FSB Handbook, Section 12.2.1, Customer Due Diligence Information and PB Handbook, Section 10.2.1, Client Due Diligence Information.

The Commission is proposing that firms keep a record or have a means to identify all relationship records where any of the described technology methods have been used.

New Rules

The proposed new rule in this section is in the grey highlighted box at point 4.

1. Regulation 14 for both financial services businesses ("FSB") and prescribed businesses ("PB") provides for the record keeping requirements of the Regulations. *(Please note that for ease of reference the copy below is a combination of FSB and PB Regulation 14).*

Regulation 14

14. (1) A <*FSB/PB*> shall keep-

(a) a transaction document and any customer <*client*> due diligence information, or

(b) a copy thereof,

for the minimum retention period.

(2) Where a <*FSB/PB*> is required by any enactment, rule of law or court order to provide a transaction document or any customer <*client*> due diligence information to any person before the end of the minimum retention period, the <*FSB/PB*> shall

(a) keep a copy of the transaction document or customer <*client*> due diligence information until the period has ended or the original is returned, whichever occurs first, and

(b) maintain a register of transaction documents and customer due diligence information so provided.

(3) A <*FSB/PB*> shall also keep records of –

(a) any reports made to a money laundering reporting officer as referred to in regulation 12 and of any disclosure made under Part I of the Disclosure Law or section 15 or 15A (*FSBs*) 12 (*PBs*) of the Terrorism Law made other than by way of a report to the money laundering reporting officer, for five years starting from-

(i) in the case of a report or a disclosure in relation to a business relationship, the date the business relationship ceased, or

(ii) in the case of a report or a disclosure in relation to an occasional transaction, the date that transaction was completed,

(b) any training carried out under regulation 13 for five years starting from the date the training was carried out,

(c) any minutes or other documents prepared pursuant to regulation 15(c) until –

(i) the expiry of a period of five years starting from the date they were finalised, or

(ii) they are superseded by later minutes or other documents prepared under that regulation,

whichever occurs later, and

(d) its policies, procedures and controls which it is required to establish and maintain pursuant to these Regulations, until the expiry of a period of five years starting from the date that they ceased to be operative.

(4) Documents and customer <client> due diligence information, including any copies thereof, kept under this regulation –

(a) may be kept in any manner or form, provided that they are readily retrievable, and

(b) must be made available promptly

(i) to an auditor, and

(ii) to any police officer, the Financial Intelligence Service, the Commission or any other person where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment.

8.1. Record- Keeping Requirements, Electronic Records

1. The record keeping requirements, detailed in the Handbook sections on Record-keeping 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.

2. Firms should include 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.

3. Retention may be:

- By way of original documents;
- On microfiche;
- In a scanned form;
- In a computer or electronic form.

8.2. Record-Keeping Requirements, Electronic Records

4. Firms must keep a record or have a means to identify all relationship records where any of the described technology methods have been used.

Index

	Questions for Respondents
1	Are there any additional areas to consider within Section 7.5, “Areas to Consider when Assessing an Electronic Method or System”?
2	Should the use of technology for due diligence purposes be restricted to low and standard risk relationships?
3	Should the use of technology for due diligence purposes be restricted to relationships originating from the UK and the Crown Dependencies?
4	Are there any other areas of the due diligence process where technology could be used and added to the described processes? If yes, please state the areas.
5	During the development of the proposals, a number of reference documents were used for information purposes. Would it be beneficial if a bibliography was included to assist compile a technical risk evaluation and/or conduct independent research?