



ISLE OF MAN
FINANCIAL SERVICES AUTHORITY
Lught-Reill Shirveishyn Argidoll Ellan Vannin

SEPTEMBER 2024

ISLE OF MAN MONEYLENDERS CDD & ECDD (INCLUDING SOF & SOW)

AML/CFT THEMATIC REPORT PHASE 1 – QUESTIONNAIRE

www.iomfsa.im



aml@iomfsa.im



Contents

1	Glossary of Terms.....	p3
2	Background.....	p4
2.1	Executive Summary.....	p4
2.2	Scope.....	p5
2.3	CDD & ECDD Obligations.....	p6
3	Phase 1 Results, Key Findings and Observations.....	p7
3.1	Sector Specific Risks.....	p8
3.2	Customer Due Diligence.....	p12
3.3	Enhanced Customer Due Diligence.....	p17
3.4	Onboarding and New Business Risks.....	p22
3.5	Natural Persons.....	p23
3.6	Legal Persons.....	p24
3.7	Legal Arrangements.....	p25
3.8	Foundations.....	p25
3.9	Electronic Methods.....	p26
3.10	Controls.....	p27
	Appendix 1.....	p34

1 Glossary of Terms

<u>TERM</u>	<u>MEANING IN THIS REPORT</u>
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
Authority	The Isle of Man Financial Services Authority
CDD	Customer Due Diligence
Code	Anti-Money Laundering/Countering the Financing of Terrorism Code 2019
CRA	Customer Risk Assessment
DBRO	Designated Businesses (Registration and Oversight) Act 2015
DNFBP	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence
Handbook	Anti-Money Laundering and Countering the Financing of Terrorism Handbook
ML/FT	Money Laundering/Financing of Terrorism
Moneylenders	Lending, Financial Leasing and Financial Guarantees businesses
ML/FT	Money Laundering/Financing of Terrorism
NRA	National Risk Assessment
Relevant Person	Means a person carrying on business in the regulated sector included in paragraphs 2(6)(a) to (t) of Schedule 4 to the Proceeds of Crime Act 2008
Registered Person	Means a person registered under section 9 of the Designated Businesses (Registration and Oversight) Act 2015
Regulated	Refers to firms regulated under the Financial Services Act 2008, the Insurance Act 2008, and the Retirement Benefits Schemes Act 2000
SOF	Source of Funds
SOW	Source of Wealth

2 Background

2.1 Executive Summary

The Authority is currently undertaking a thematic project involving Moneylenders on the Isle of Man. The sector is considered one of the lower risk business areas with regards ML/FT risk on the Isle of Man. The Authority initially gathered data and information from Moneylenders, to review how relevant persons have met and undertaken their obligations regarding CDD and ECDD, to include SOF and SOW requirements, as laid out within the Code.

The Authority's regulatory objectives are:

- securing an appropriate degree of protection for policyholders, members of retirement benefits schemes and the customers of persons carrying on a regulated activity;
- the reduction of financial crime; and
- the maintenance of confidence in the Island's financial services, insurance and pensions industries through effective regulation, thereby supporting the Island's economy and its development as an international financial centre.

A key part in achieving these objectives is the Authority's oversight and supervisory functions, which encompasses undertaking supervisory inspections and thematic reviews.

The focus of this thematic being on CDD and ECDD, to include SOF and SOW, was selected due to the importance of these concepts in terms of

CDD/ECDD helps to:

- protect the relevant person and the integrity of the Isle of Man regulated sectors (per Schedule 4 of the Proceeds of Crime Act 2008) by reducing the likelihood of relevant persons becoming a vehicle for, or victim of, other financial crime;
- assist law enforcement by providing available information on customers or activities, funds or transactions being investigated; and
- guard against identity theft.



relevant persons' AML/CFT regimes. The purpose of CDD and ECDD in the AML/CFT context is to ensure relevant persons know, as far as reasonably possible, who they are dealing with, and the ML/FT risks associated with that customer.

Robust CDD/ECDD procedures and controls are designed to ensure that relevant persons are aware of the potential ML/FT risks posed by customers at the outset, and for the duration of, the business relation-

ship/occasional transaction.

It is only with robust CDD/ECDD procedures and controls that relevant persons can meet the requirements of the AML/CFT legislation effectively, and are in a position to forestall abuse of the financial system by criminals or by those who would seek to use it for terrorism purposes.

CDD/ECDD is integral to managing and mitigating ML/FT risks, as without satisfactory CDD/ECDD, it is not possible to conduct effective risk assessments, monitor business relationships/transactions for unusual or suspicious activity, or make meaningful and comprehensive disclosures of suspicions to the Isle of Man Financial Intelligence Unit.

CDD and ECDD are integral to managing and mitigating ML/FT risks

The planning for this thematic project began in late 2023 and the background was shared in a **public statement** released on the Authority's website in April 2024. The statement notified Moneylenders of the upcoming thematic which was to commence in 2024.

"The moneylending sector is a supervised sector in respect of AML/CFT/CPF and this thematic exercise presents a great opportunity to gain a better overview of the varied and wide sector on the Island, as part of the review and refresh of ML, TF and PF risk assessments for the Isle of Man.

"As the Authority aims to work closely with the sector, this thematic allows us to test and evidence how super-

vised entities are meeting their AML/CFT obligations.

"Through increased engagement with businesses during the project and as we progress, we hope to discover and highlight some best practice which can be shared with the wider industry, through our public thematic reports, as well as updating the sector specific guidance."

The thematic exercise is made up of two core phases. Phase 1 of the thematic consisted of a CDD and

ECDD questionnaire issued via STRIX to 37 Moneylenders for completion, following a selection process detailed below in section 2.2. This report will outline the results from this first phase, as well as the Authority's observations on the data.

Phase 2, which commenced in July 2024, consists of inspections focusing on CDD and ECDD. The Moneylenders CDD and ECDD thematic project is expected to conclude during 2025, where subsequently a Phase 2 report will be issued.


Phase 2 of the review will consist of inspections focusing on CDD and ECDD

2.2 Thematic Scope

Prior to the Phase 1 questionnaire being issued, information and data on all 38 Moneylenders registered with the Authority was collated and analysed. As part of this, the Authority considered the outcomes of recent supervisory inspections, as well as the data from relevant persons' AML/CFT annual statistical returns.

The Authority then excluded any Moneylenders in the process of being de-registered as a DNFBP with the Authority. 37 firms were ultimately selected for inclusion in Phase 1 of the thematic.

After further analysis of the gathered data against the prescribed risk parameters and the Phase 1 outcomes, an initial cohort of 21



Recent inspections and returns data were considered prior to issuing the Phase 1 questionnaire.

Moneylenders has been selected to form Phase 2 of the thematic. Phase 2 will involve focused inspections to test and evidence firms' compliance with the Code in relation to CDD and ECDD. Given the large scale of

this thematic and time it will take to complete, the number of Moneylenders in Phase 2 is expected to fluctuate as the thematic progresses, where Moneylenders may be added or removed as time progresses.

Initial Planning -
38 Moneylenders

Phase 1 -
37 Moneylenders

Phase 2 -
21* Moneylenders

*Phase 2 is ongoing and may fluctuate; this is a provisional figure only.

2.2 AML/CFT Code 2019 - CDD & ECDD Obligations

The focus and primary objectives of this thematic project are paragraphs 4, 8 and 15 of the Code. For ease, extracts of paragraphs 8 and 15 of the Code can be found at [Appendix 1](#) of this report, on page 34.

The Handbook also provides a variety of additional guidance around paragraphs 4, 8 and 15 of the Code including the following useful extracts. For any further guidance please consult [the Code](#) and [the Handbook](#) in full.

Handbook quote:

3.4.7: Enhanced Customer Due Diligence (“ECDD”)

Enhanced requirements are relative to what the relevant person already does as standard meaning it is for relevant persons to determine what ECDD is appropriate on a case-by-case basis taking into account the higher ML/FT risk and the overarching requirement that their procedures and controls must enable them to manage and mitigate the higher ML/FT risks.

Enhancements of the standard CDD and ongoing monitoring requirements and the standard procedures and controls established and maintained by each relevant person include obtaining more information/documentation, to a broader degree or a greater depth, more frequently.

In respect of enhanced/additional ongoing monitoring this could include obtaining information on the reasons for intended or performed transactions, increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

Handbook quote:

3.5 Identifying the customer, beneficial owner and other related parties

The risk-based approach allows flexibility in respect of the extent of identity information to obtain on a case-by-case basis, subject to other legal (including AML/CFT) obligations, a relevant persons’ risk assessments and provided ML/FT risks are effectively managed and mitigated. Consequently, where there are higher ML/FT risks, relevant persons must consider whether additional identity information is needed and obtain it.

It is for relevant persons to make their own reasoned judgements in any particular case as to the extent of identity information to gather, and it is for relevant persons to ensure they can justify their decisions. Adequately recording the decisions taken as well as the reasons for the decisions is essential in enabling relevant persons to do this.



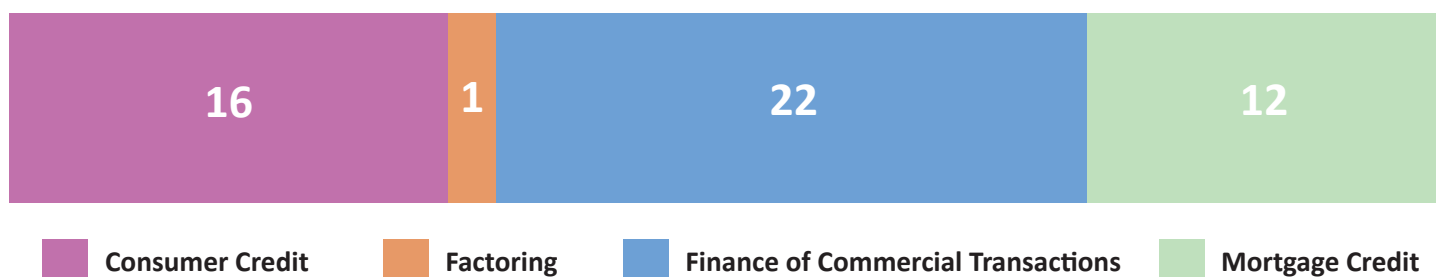
3 Phase 1 CDD & ECDD Questionnaire Results, Key Findings and Observations

Q1, Q7, Q9: Breakdown of the Moneylenders sector by permission(s) held:



All Moneylenders included in Phase 1 reported as being registered as a Lender, whilst only four firms were additionally registered for Financial Leasing and one firm was registered for Financial Guarantees, meaning that this firm was registered with all three Moneylender permissions.

Q3, Q4, Q5, Q6: Lending offerings provided:

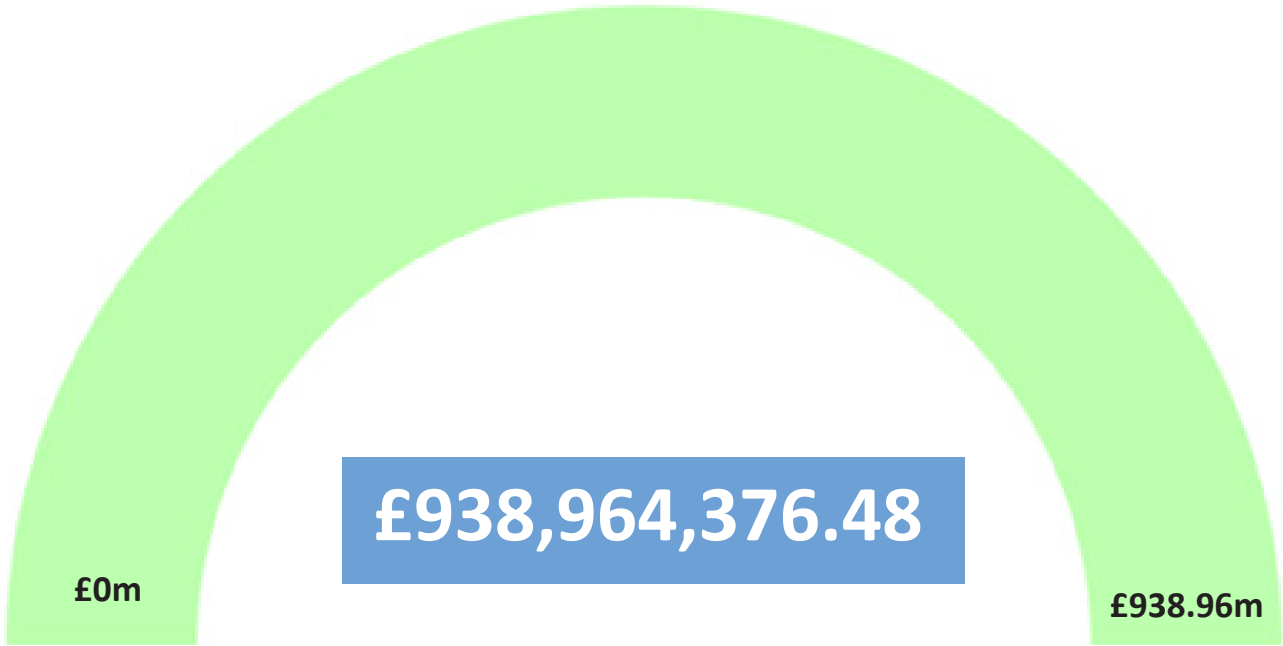


- 22 Moneylenders (59%) reported that they provide the finance of commercial transactions services as part of the lending offerings.
- 16 Moneylenders (43%) reported that they provide consumer credit services as part of their lending offerings.
- 12 Moneylenders (32%) reported that they provide mortgage credit services as part of their lending offering.
- 1 Moneylender (3%) reported that they provide factoring services as part of their lending offering.

Q2: Total customers serviced by the 37 Moneylenders included in Phase 1:

5,383 customers

Q11: Total value of finance outstanding on all existing customers as at 31 December 2023 between all 37 Moneylenders included in Phase 1:



3.1 Sector Specific Risks

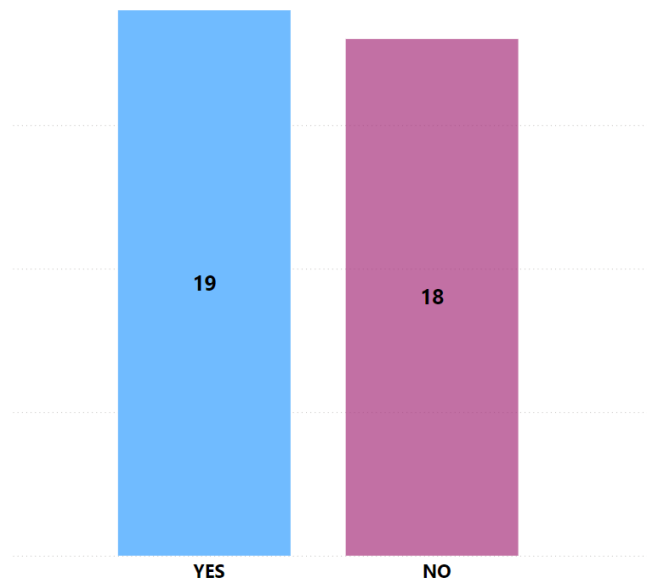
Q12: Do you allow shortened or reduced repayment schedules within a customer relationship

Of the total 37 Moneylenders, answers to this question provided an almost even split with 19 responding with “Yes” that shortened or reduced repayment schedules are accepted, and 18 responding with “No”.

The Isle of Man’s NRA 2020 sets out the following:

“Typology reports indicate that the most common vulnerability faced by lenders is where cash is drawn down from the provider and then repaid with the proceeds of crime, either very quickly afterwards or over a short repayment period. This allows for the exchange of criminal proceeds with clean money from the loan provider and provides the criminal with documented evidence of a seemingly legitimate source of funds. Early repayments carry a risk that the funds have emanated from a criminal lifestyle”.

Moneylenders should ensure that where shortened or reduced repayment schedules are allowed, that the risk

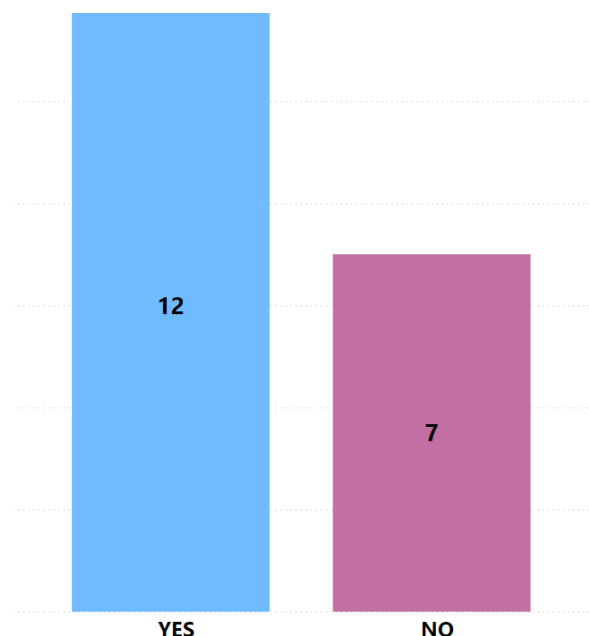


profile of the customer is thoroughly considered, and that where these are permitted, the rationale is understood and deemed acceptable.

Q13: Do you consider shortened or reduced repayment schedules as part of the customer risk profile?

Of the 19 Moneylenders who confirmed they allow customers to utilise shortened or reduced repayment schedules, 12 responded “Yes” advising that they consider shortened or reduced repayment schedules as part of the customer risk profile. 7 Moneylenders responded “No” advising that these risks are not considered as part of the customer risk profile.

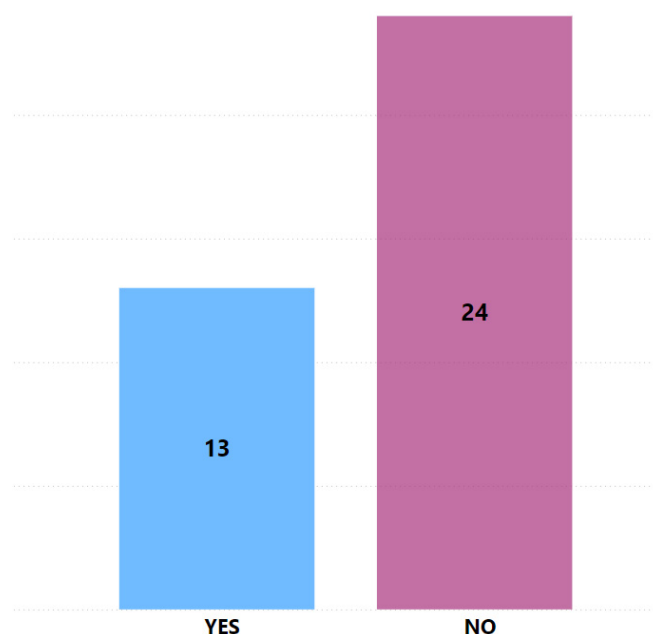
Paragraph 6(3) of the Code requires a customer risk assessment to consider all relevant risk factors. As this is a sector specific risk identified within the Isle of Man’s NRA, the Authority would expect to see shortened or reduced repayment schedules considered as a relevant risk factor.



Q14: Do you allow third party repayments within a customer relationship?

13 of the 37 Moneylenders responded “Yes” to this question, confirming that they allow third party repayments within a customer relationship. However, the majority of Moneylenders advised that they do not accept third party repayments, with 24 answering “No”.

The Sector Specific Guidance for Moneylenders issued in August 2021¹ sets out that repayments are expected to normally be made from the customer’s own bank or building society account by direct debit or bank transfer. Where the lender accepts occasional payments from third parties it must ensure that the source of these funds is determined in accordance with the Code, and establish the relationship between its customer and the third party.



Repayments are expected to normally be made from the customer’s own bank or building society account by direct debit or bank transfer.

¹ <https://www.iomfsa.im/media/2859/moneylenders-and-providers-of-financial-guaranteecommitments-sector-specific-amlcft-guidance-notes.pdf>

Q15-18: Do you consider third party repayments as part of the customer risk profile? Do you verify the identity of such third parties? Do you conduct ECDD where necessary on such third parties? Are the reasons for a third party repayment recorded?

Of the 13 Moneylenders who confirmed that they allow third party payments within a customer relationship:

- 8 Moneylenders advised that they consider the third party repayments as part of the customer risk profile.
- 13 Moneylenders advised that they verify the identity of the third parties.
- 12 Moneylenders advised that they conduct ECDD on the third parties where necessary.



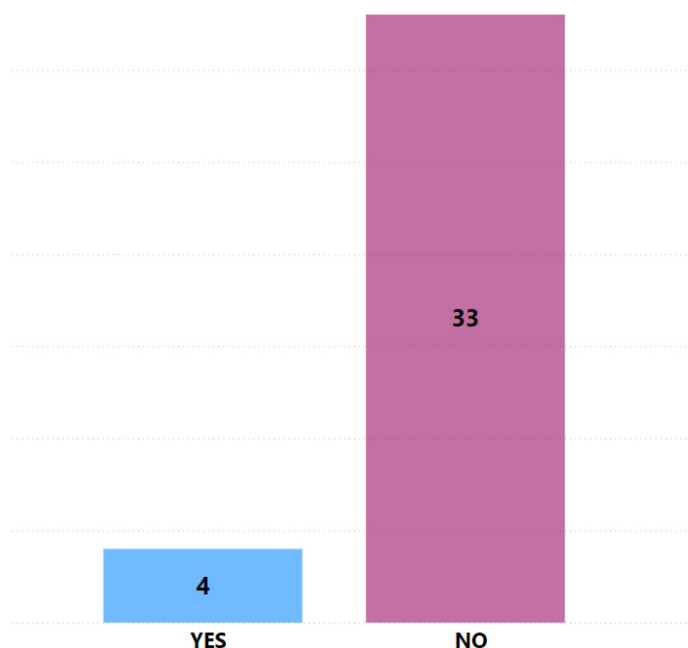
- 13 Moneylenders advised that the reasons for the third party repayment are recorded.
- Paragraph 8(3)(e) of the Code lays out the requirements of a relevant person where the funds are received

from an account not in the name of the customer, including understanding and recording the reasons, identifying and taking reasonable measures to verify the account holder, and undertaking ECDD as appropriate.

Q19: Do you accept cash repayments within a customer relationship?

The majority of respondents, 33 of 37 Moneylenders, answered “No”, advising that they do not accept cash repayments. However, there is a small proportion that do accept cash repayments within a customer relationship with 4 responding “Yes” to this particular question.

Repayments in cash present an inherent money laundering risk as providing verification of the source of the cash can be difficult. The Sector Specific Guidance goes as far as stating that cash repayments should not be encouraged given the risks posed.

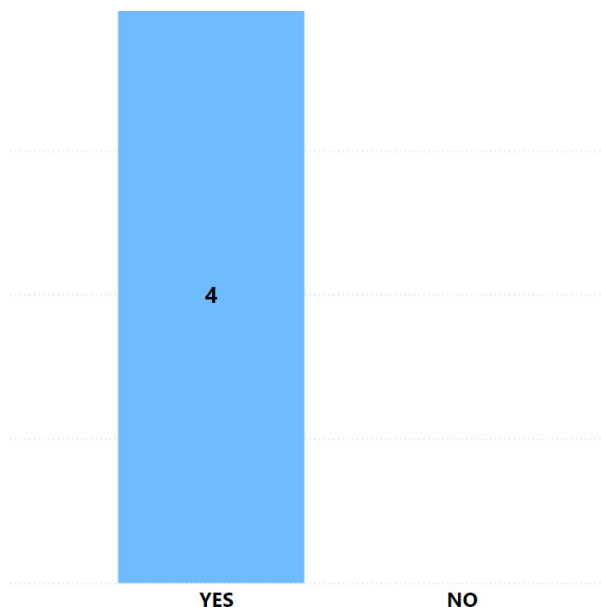


Sector Specific Guidance goes as far as stating that cash repayments should not be encouraged given the risks posed

Q20 and Q21: Do you consider cash repayments as part of the customer risk profile? Number of customer relationships whereby cash repayments have been accepted during the reporting period (01/01/2023 to 31/12/2023)?

Of the 4 Moneylenders who advised that they accept cash repayments within a customer relationship, all 4 Moneylenders confirmed that they consider cash repayments as part of the customer risk profile.

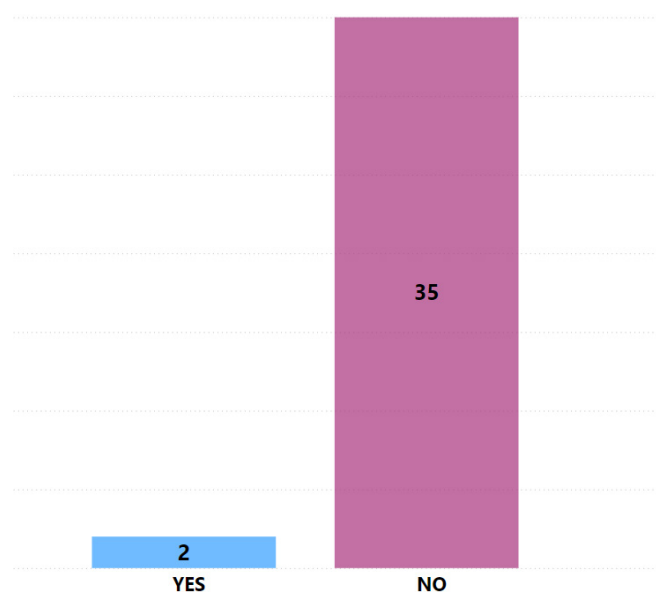
The questionnaire also asked those accepting cash repayments within a customer relationship to provide the number of customer relationships whereby cash repayments had been accepted during the reporting period. Between the 4 Moneylenders, 23 customer relationships were reported as having utilised cash repayments.



Q22: Do you accept prepaid cards as a method of repayment within a customer relationship?

The majority of Moneylenders do not accept prepaid cards as a method of repayment within a customer relationship, with 35 respondents answering “No” to this question. Only 2 respondents answered “Yes”.

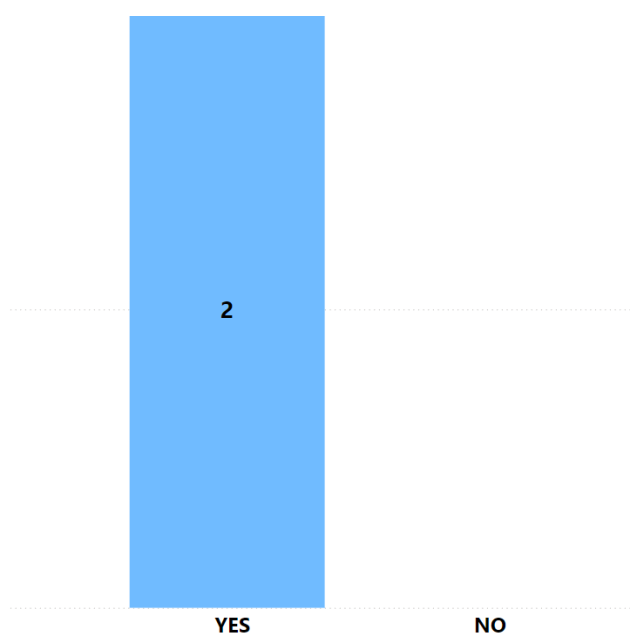
Prepaid cards may present a higher inherent risk as they can be loaded with illicit funds or used anonymously².



Q23 and Q24: Do you consider prepaid card repayments as part of the customer risk profile? Number of customer relationships whereby prepaid card repayments have been accepted during the reporting period (01/01/2023 to 31/12/2023)

Of the 2 Moneylenders who advised that they accept prepaid cards as a method of repayment within a customer relationship, both confirmed that they consider prepaid card repayments as part of the customer risk profile.

The questionnaire also asked those accepting prepaid card repayments within a customer relationship to provide the number of customer relationships whereby prepaid card repayments had been accepted during the reporting period. Between the 2 Moneylenders, 11 customer relationships were reported as having utilised prepaid card repayments.



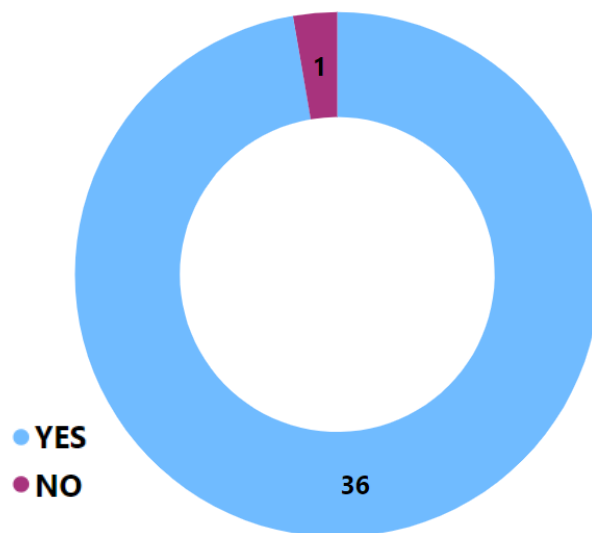
² <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-NPPS.pdf.coredownload.pdf>

3.2 Customer Due Diligence

Q25: Do you conduct CDD on all customers involved in a business relationship?

36 out of the 37 respondents answered with “Yes” to this question confirming that they conduct CDD on all customers involved in a business relationship. Only 1 Moneylender answered “No”. It has subsequently been identified that this “No” answer was a submission error rather than a true reflection of the position taken in relation to CDD by this particular lender³.

CDD is fundamental to the on-boarding process of a customer and its purpose is to ensure that the business understands who they are dealing with, and the ML/TF risks of dealing with that customer. Conducting CDD involves obtaining, documenting and using a broad range of information relating to a customer relationship or occa-



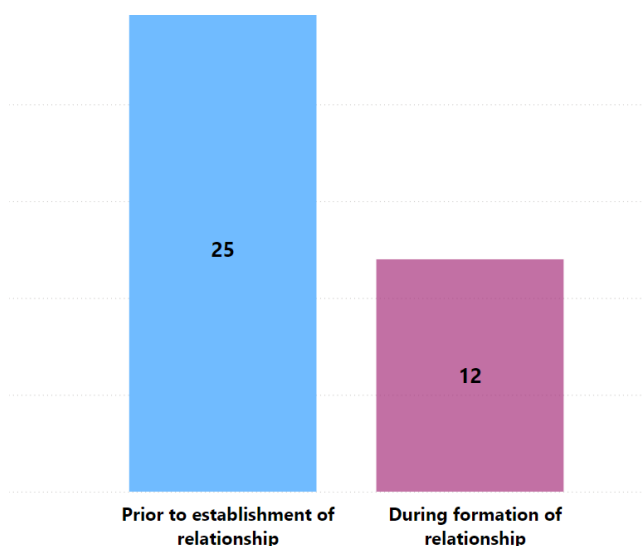
sional transaction. Further information is detailed in the Handbook.

Q26: When is CDD typically first obtained on a customer during a business relationship?

25 of the 37 respondents obtain CDD prior to the establishment of the relationship with the remaining 12 doing so during the formation of the relationship. Both of these answers satisfy the requirements of the Code.

The Handbook sets out that;

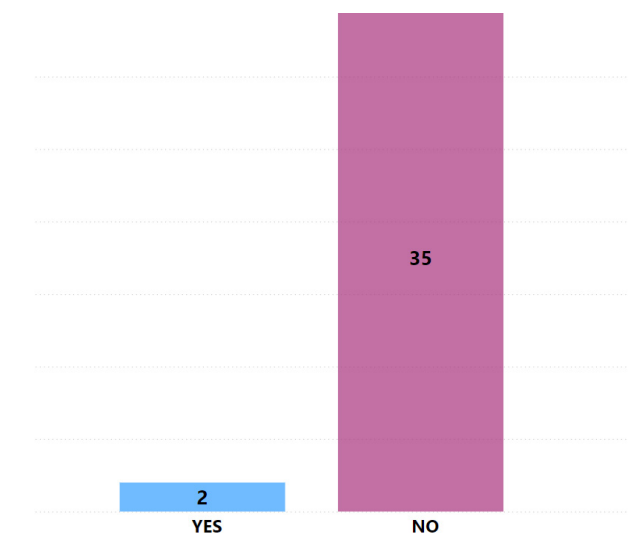
“Initial CDD must be undertaken before a business relationship / occasional transaction is entered into or during the formation of that relationship”. This initial CDD is what allows the relevant person to accurately undertake the initial CRA, and in turn determines if additional CDD or EDD information or documentation is required.



Q27: Are there any cases where CDD has been obtained after the formation of a relationship?

The majority of respondents, 35 of the 37, answered “No” to this question, advising that they had no cases where CDD had been obtained after the formation of a relationship. However 2 respondents answered “Yes”.

Paragraph 8(2) of the Code requires a relevant person to undertake elements of CDD prior to the relationship being entered into, or during the formation of that relationship. There are a limited circumstances laid out at paragraph 8(4) of the Code which allows the verification of the identity of the customer to take place after the formation of the business relationship.



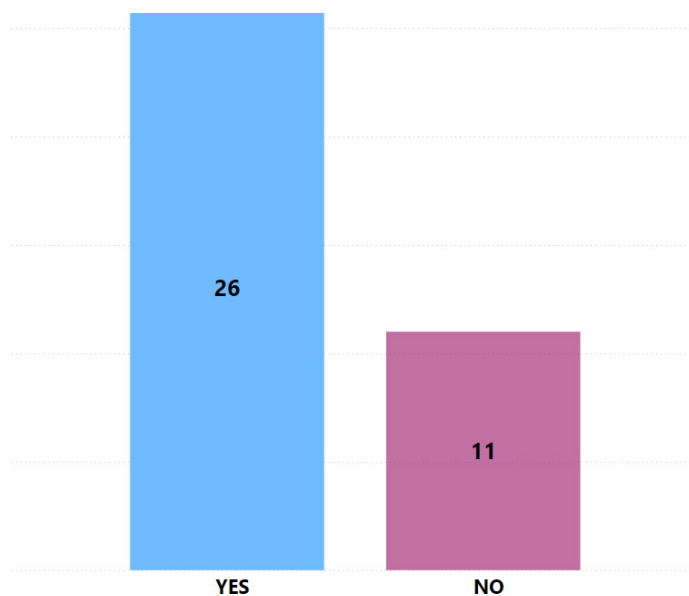
³ Due to this reporting error, answers to questions 29-36 inclusive may not be truly representative of the sector.

Q28: Do you use electronic methods as part of the CDD/ECDD process?⁴

26 “Yes” responses indicate that the majority of Money-lenders permit the use of electronic methods as part of the CDD/ECDD process.

The Code and the Handbook are technology neutral and as such the use of technology in respect of CDD obligations is permitted.

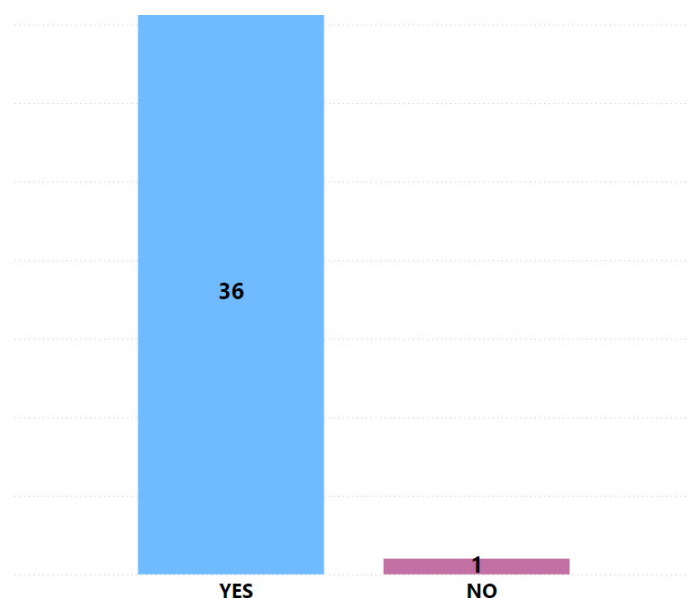
The use of technology as part of the CDD process should be sufficiently risk assessed within the technology risk assessment as required by paragraph 7 of the Code.



Q29: As part of CDD do you identify the customer?

36 out of the 37 Moneylenders responded with “Yes”, confirming that as part of CDD they identify the customer. As noted at Q25, it has been identified that the 1 respondent answering “No” was a completion error during the questionnaire submission.

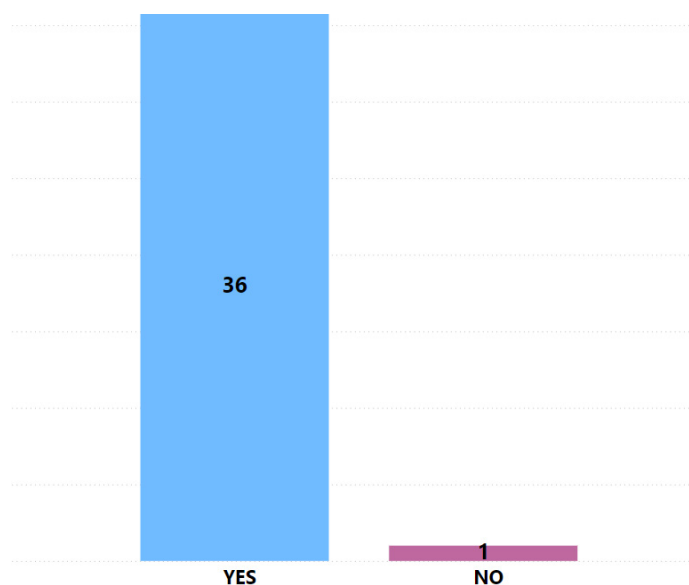
Identification of a customer is a requirement under paragraph 8(3) of the Code and therefore the relevant persons must identify the customer to be able to demonstrate compliance.



Q30: As part of CDD do you verify the identity of the customer?

36 respondents answered “Yes” to this question, confirming that as part of CDD they verify the identity of the customer. Again, it is understood that the 1 “No” response was a submission error when completing the questionnaire.

Verification of the identity of the customer is about taking steps to check that the customer is who they say they are, and can include examining the authenticity and validity of any information or documentation gathered; this is a requirement under paragraph 8(3) of the Code.

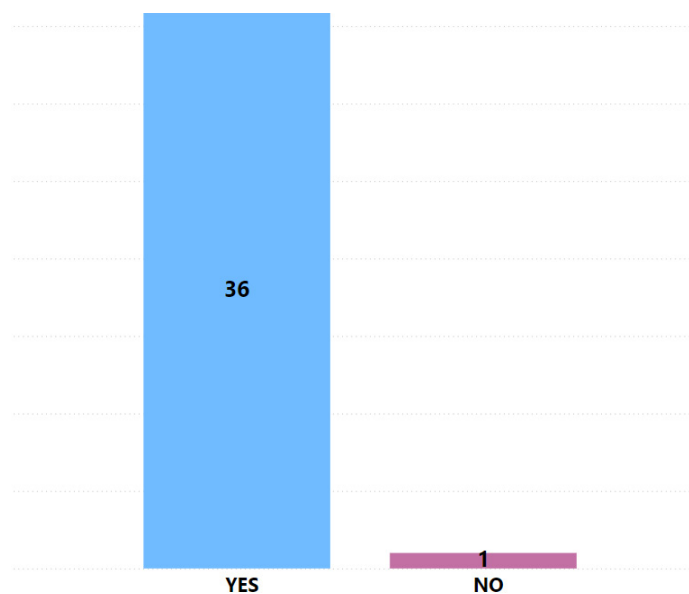


⁴ This includes the use and analysis of electronic databases and open source information to know your customer, e.g. electoral registers, as well as electronic verification providers and KYC utilities.

Q31: As part of CDD do you verify the address of the customer?

36 respondents answered “Yes” to this question, confirming that as part of CDD they verify the address of the customer. Again, it is understood that the 1 “No” response was a submission error when completing the questionnaire.

Verification of the of the customer’s address is a part of taking steps to check the customer is who they say they are.

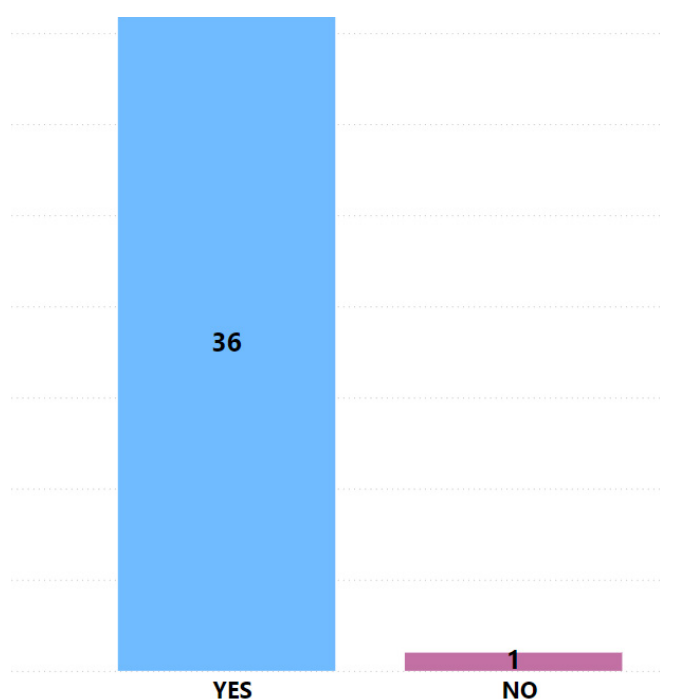


Q32: As part of CDD do you obtain the nature and intended purpose of the business relationship?

36 respondents answered “Yes” to this question, indicating that as part of CDD the nature and intended purpose of the business relationship is obtained. Again, it is understood that the 1 “No” response was a submission error when completing the questionnaire.

Obtaining information on the nature of purpose of the business relationship a requirement of paragraph 8(3) of the Code, and is a crucial element of the CDD process as it allows the relevant person to identify any unusual activity that may transpire during the course of the relationship.

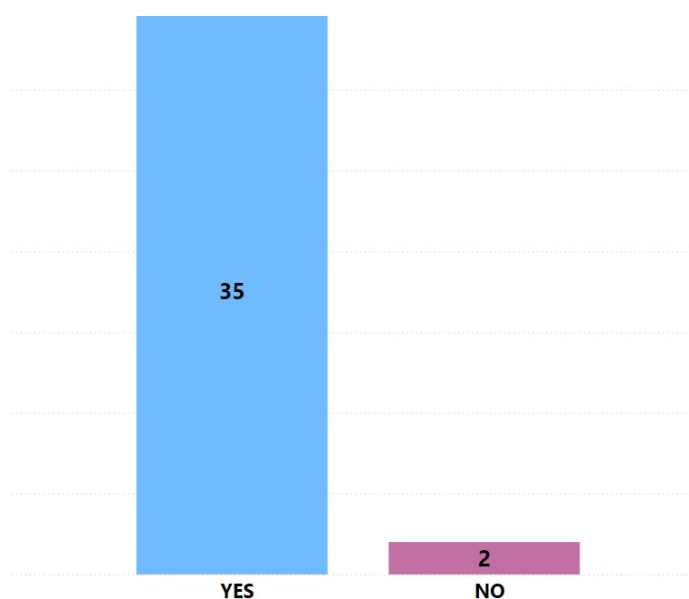
If a customer is reluctant to provide information or only provides minimal information with regard to the nature and purpose of the relationship, including the purpose of the loan, this may be considered a red flag and appropriate steps should be taken to ensure that the business does not proceed further and any suspicions are reported.



Q33: As part of CDD do you verify the legal status of the customer?

35 respondents answered “Yes” to this question, confirming that as part of CDD they verify the legal status of the customer. Again, it is understood that 1 of the “No” responses to this question was a submission error when completing the questionnaire.

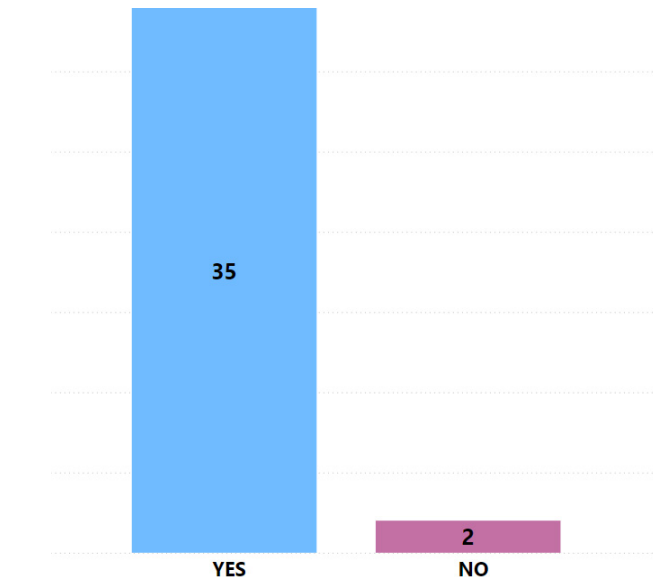
Verifying the legal status of the customer is required by paragraph 8(3) of the Code and applies to all types of customer. The Handbook gives examples of what this would require for a legal person, e.g. verification of the type of legal person and its current status; live or otherwise. For the legal status of a legal arrangement this would involve verification of the trustees and the nature of their duties.



Q34: As part of CDD do you establish the origin of the particular funds or other assets involved in a business relationship or occasional transaction and the means through which the funds were transferred (e.g. bank account, sort code, account holder’s name)?

35 respondents answered “Yes” advising that as part of CDD they establish the origin of the particular funds or other assets involved in a business relationship or occasional transaction and the means through which the funds were transferred. 2 respondents answered “No” to this question. Again, it is understood that 1 of the “No” responses to this question was a submission error when completing the questionnaire.

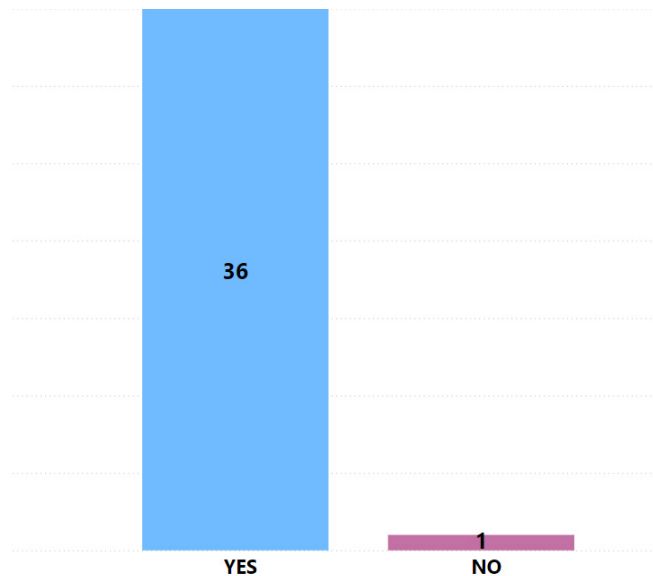
SOF is a twofold concept comprising the activity that generated the funds and the means through which the funds are transferred. Source of funds, e.g. the funds being repaid to lenders, is a key element of the CDD process. It enables the relevant person to identify ML/TF risks posed by the



customer and understand more about the customer’s background. It should also be used to verify that repayments are originating from the expected account associated with the customer.

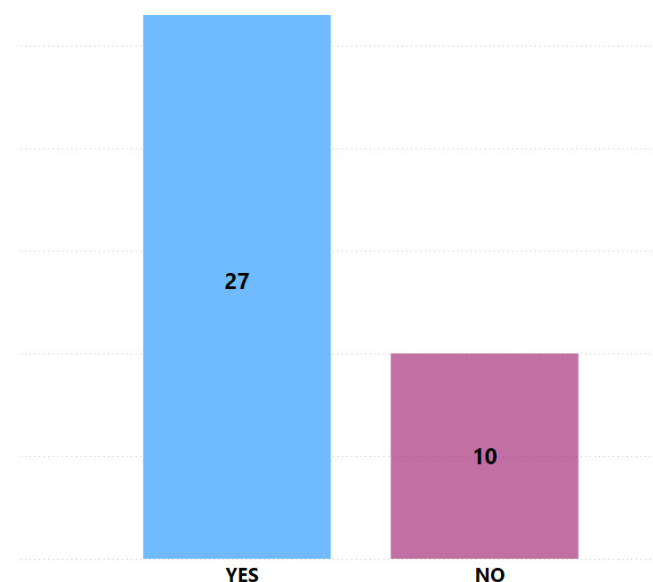
Q35: As part of CDD do you establish the activity that generated the funds used in the business relationship or occasional transaction:

36 respondents answered “Yes” to this question, confirming that as part of CDD they establish the activity that generated the funds used in the business relationship or occasional transaction. Again, it is understood that the 1 “No” response to this question was a submission error when completing the questionnaire. As mentioned at Q34, SOF information should comprise of both the activity that generated the funds and account the funds are being remitted from.



Q36: As part of CDD do you conduct screening on the customer and any other relevant parties (e.g. using WorldCheck, RiskScreen, Dow Jones)?

27 respondents answered “Yes” confirming that as part of CDD they conduct screening on the customer and any other relevant parties. 10 Moneylenders answered “No” to this question. It is understood that 1 of the “No” responses to this question was a submission error when completing the questionnaire. Screening, when undertaken as part of the CDD process, may identify sanctions hits, PEP information, criminal history or negative press that may impact the risk profile and suitability of the applicant. Alternatively, results produced via screening could help support the identity information or documentation provided and be used as an independent source to help verify its credibility.

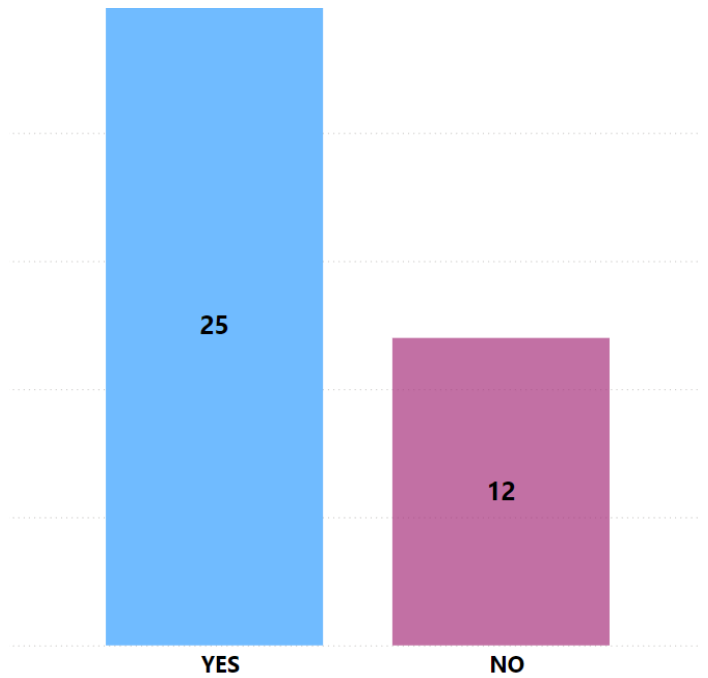


Q37: As part of CDD do you conduct open source adverse media checks on the customer and any other relevant parties?

25 respondents confirmed that as part of CDD they conduct open source adverse media checks on the customer and any other relevant parties by answering “Yes” to this question. 12 respondents answered “No”.

The use of open source internet searches for adverse media will assist the relevant person with determining if the customer or potential customer fits their risk appetite, as well as impacting the risk profile of the customer within the CRA. It is important to fully understand and document the risks associated with a customer to ensure that the appropriate level of mitigation is in place to prevent the risk of ML/TF transpiring.

- Further guidance on open source checks is available within the Handbook.

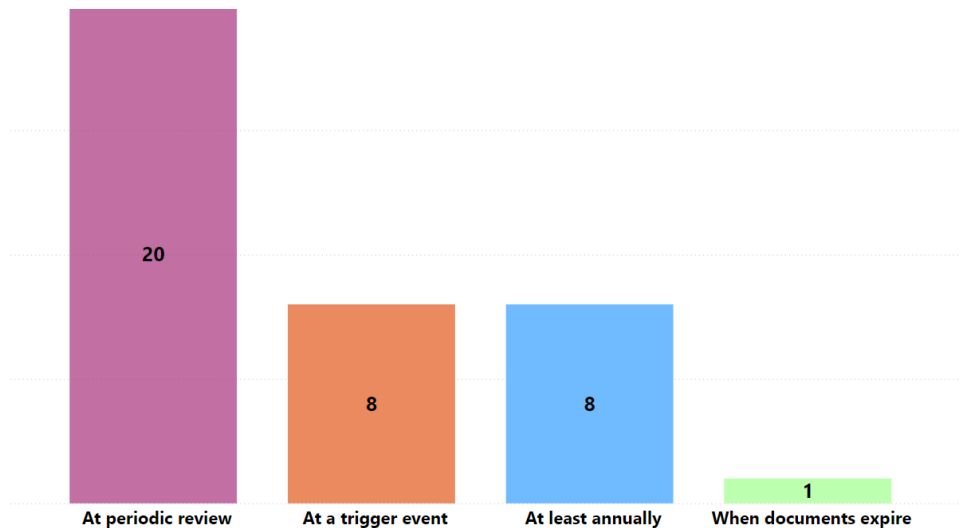


Q38: How often is CDD reviewed?

The bar chart shows the frequency at which the respondents review CDD, with the majority, 20 of the 37 Moneylenders, selecting the at periodic review option.

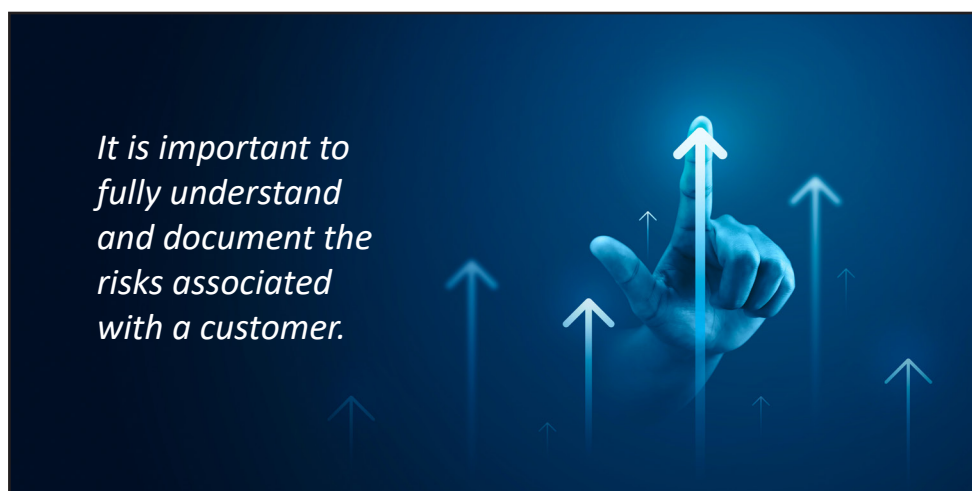
The next most common answers were the at a trigger event and the at least annually options, with 8 respondents selecting each of these answers. Only 1 Moneylender selected the “when documents expire” answer to this question.

The Handbook states that in circumstances where the customer is determined to present a lower risk of ML/TF, the frequency of CDD reviews



could potentially be carried out only as a result of a trigger event. However, it is emphasised that relevant

persons should not interpret this to mean that the CDD information is never reviewed or updated.

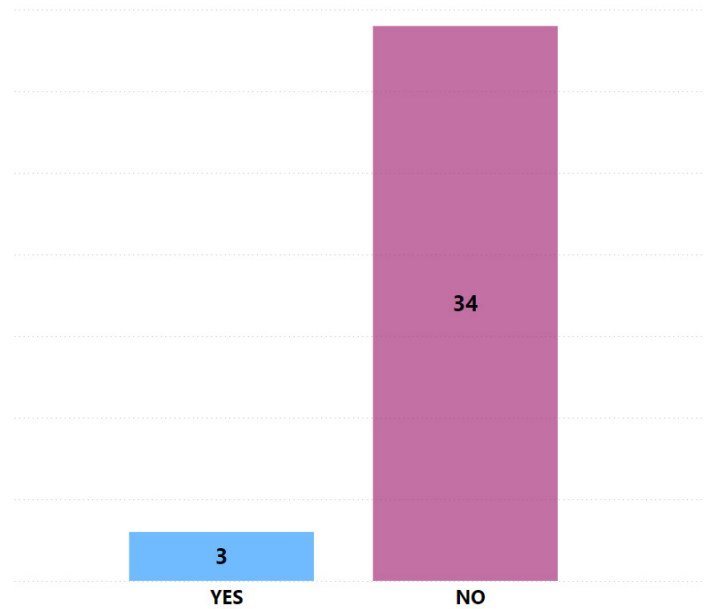


3.3 Enhanced Customer Due Diligence

Q39: Do you conduct ECDD on all customers involved in a business relationship?

Of the 37 responses, 3 relevant persons responded with a “Yes” to conducting ECDD on all customers involved in a business relationship, whilst 34 responded with “No”.

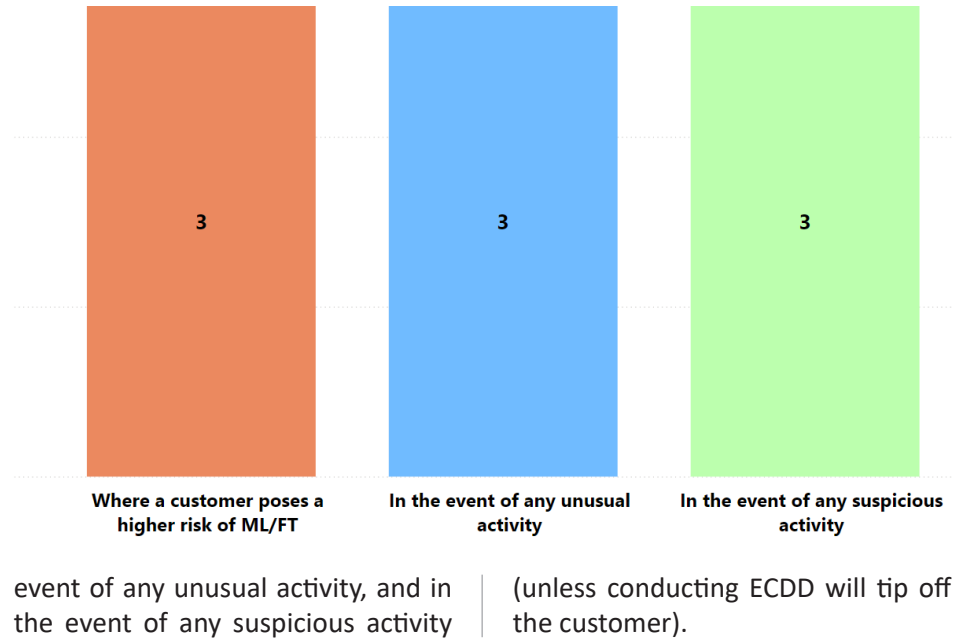
Paragraph 15(3) of the Code lays out the minimum circumstances where a relevant person is required to conduct ECDD.



Q40-42: Do you conduct ECDD where a customer poses a higher risk of ML/FT, in the event of any unusual activity and in the event of any suspicious activity (unless conducting ECDD will tip off the customer)?

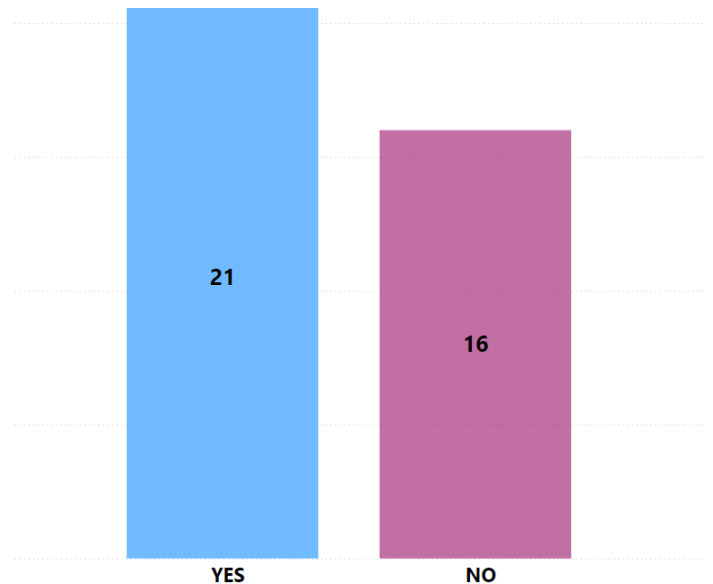
These three circumstances are the minimum requirements laid out at paragraph 15(3) of the Code where a relevant person must conduct enhanced customer due diligence.

All 3 respondents who answered “Yes” to Q39 confirmed that they conduct ECDD where a customer poses a higher risk of ML/FT, in the



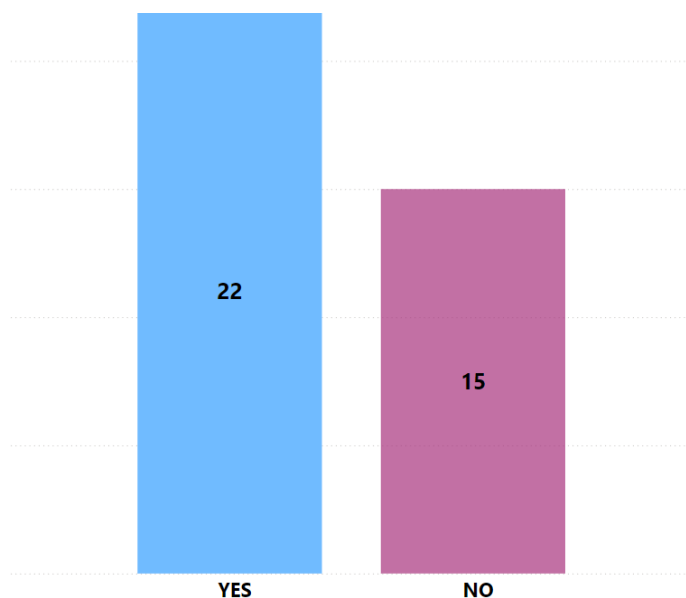
Q43: As part of ECDD do you obtain additional identification information?

21 respondents answered “Yes” indicating that they obtain additional identification information as part of ECDD, whilst 16 respondents answered “No” to this question.



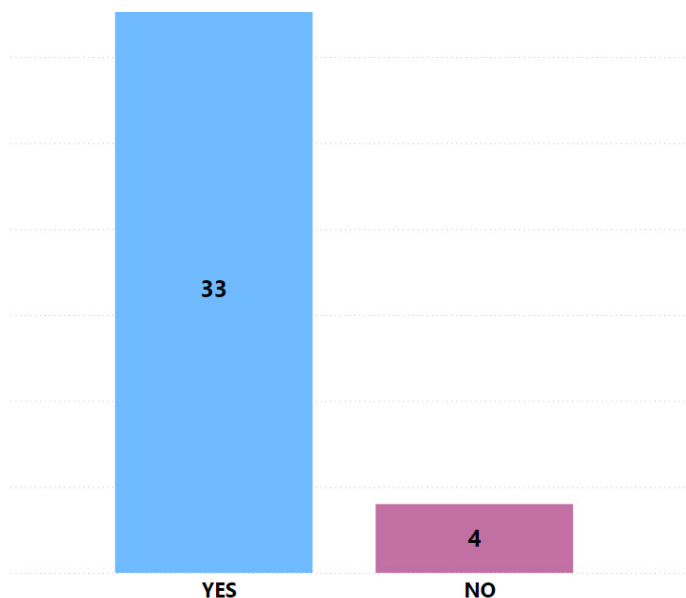
Q44: As part of ECDD do you conduct additional verification of a customer's identity?

22 respondents answered "Yes" advising that as part of ECDD they conduct additional verification of a customer's identity whilst 15 respondents answered "No" to this question.



Q45: As part of ECDD do you undertake further research in order to understand the background of a customer and a customer's business?

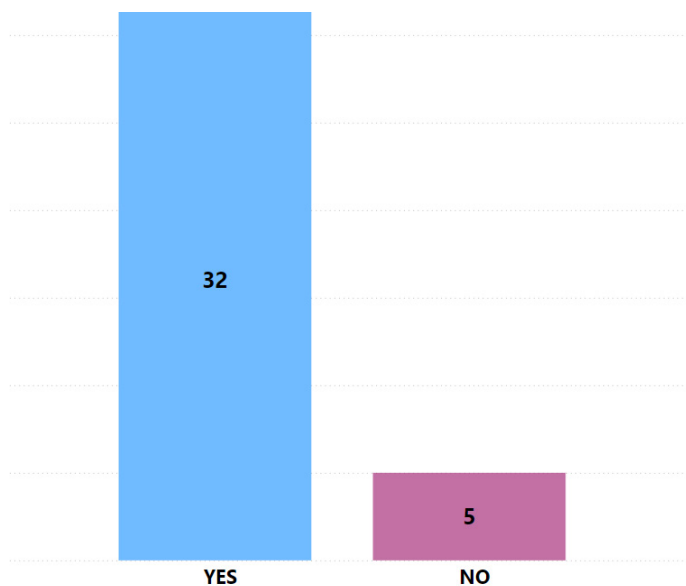
The majority of respondents answered "Yes" to this question, stating that as part of ECDD they undertake further research in order to understand the background of a customer and a customer's business. Only 4 respondents answered "No" advising that they do not undertake such further research as part of ECDD.



Q46: As part of ECDD do you establish SOW?

32 respondents answered "Yes" to this question advising that as part of ECDD they would establish a customer's SOW; only 5 respondents indicated that they do not do this.

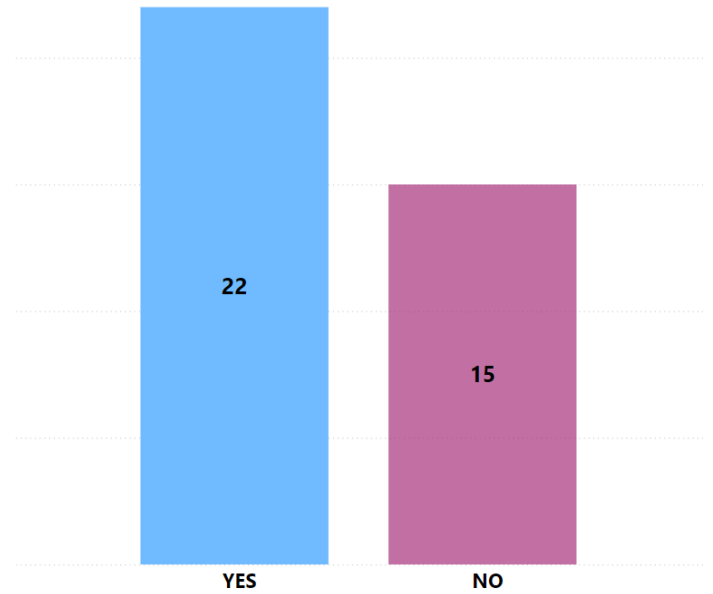
Paragraph 15(2)(c) of the Code requires a relevant person to take reasonable measures to establish the SOW of a customer as part of ECDD.



Q47: As part of ECDD do you conduct any additional transaction monitoring?

22 respondents answered “Yes” confirming that they conduct additional transaction monitoring as part of ECDD, whilst 15 respondents answered “No” advising that they do not do this.

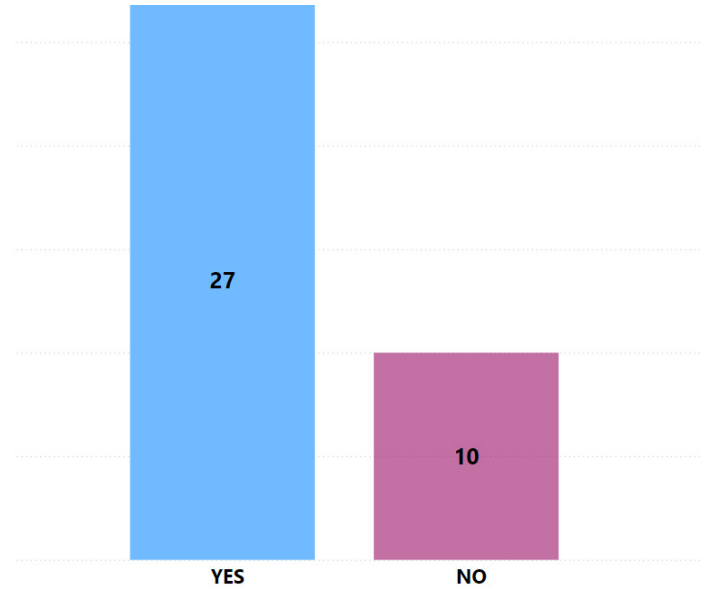
Additional transaction monitoring may be appropriate in line with paragraph 15(2)(e) of the Code which requires a relevant person to consider what additional ongoing monitoring should be carried out on a customer relationship as part of ECDD.



Q48: As part of ECDD do you conduct ongoing screening (e.g. using WorldCheck, RiskScreen, Dow Jones)?

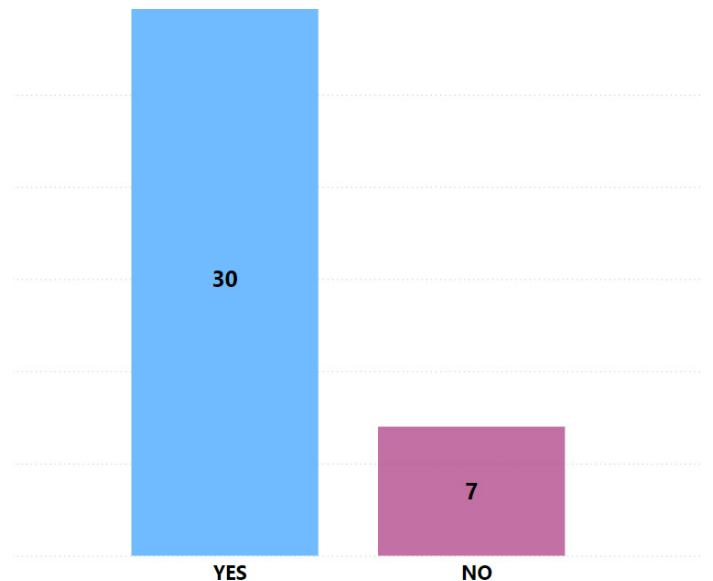
27 respondents confirmed that as part of ECDD they conduct ongoing screening by answering “Yes” to this question. 10 respondents advised that they do not do this as part of ECDD by answering “No” to this question.

Monitoring whether a customer, beneficial owner, beneficiary, introducer or eligible introducer is listed on the sanctions list is required by paragraph 13(1)(b) of the Code. In line with paragraph 15(2)(e) of the Code which requires a relevant person to consider what additional ongoing monitoring should be carried out on a customer relationship as part of ECDD, relevant persons may consider it appropriate to carry out their ongoing screening on a more frequent basis.



Q49: As part of ECDD do you conduct ongoing adverse media searches (e.g. using Google or Internet Explorer search engines)?

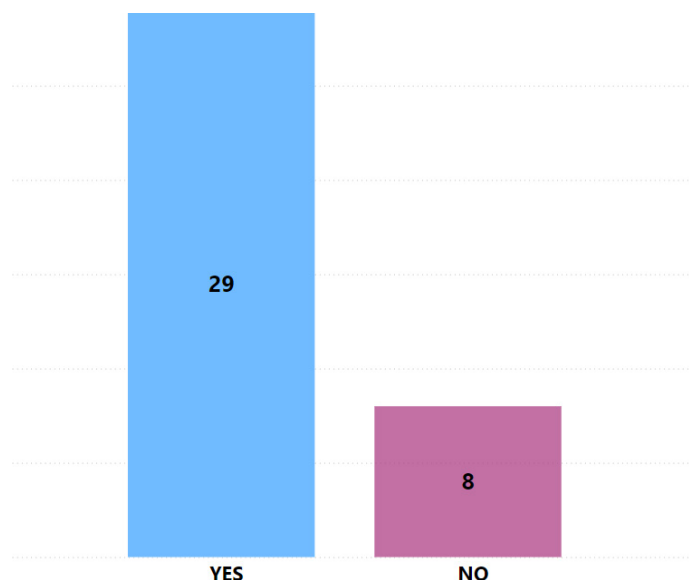
30 respondents confirmed that as part of ECDD they conduct ongoing adverse media searches, for example using Google or Internet Explorer search engines). 7 respondents confirmed they do not conduct ongoing adverse media searches as part of ECDD.



Q50: As part of ECDD do you conduct enhanced periodic customer reviews?

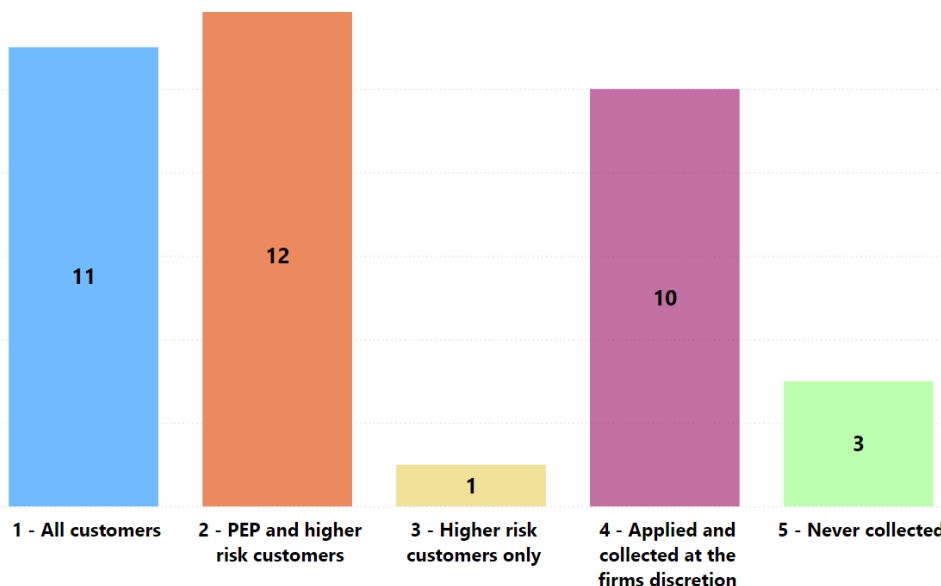
29 respondents advised that they conduct enhanced periodic customer reviews as part of ECDD, however 8 respondents advised that they do not do this.

In line with paragraph 15(2)(e) of the Code which requires a relevant person to consider what additional ongoing monitoring should be carried out on a customer relationship as part of ECDD, a relevant person may consider it appropriate to conduct enhanced periodic customer reviews.



Q51: For what type of customer is SOW required to be established (SOW means the origin of a customer's entire body of wealth and includes the total assets of the customer)?

- 11 of the 37 respondents confirmed that they require SOW to be established for all customers.
- 12 of the 37 respondents confirmed that they require SOW to be established for all PEP and higher risk customers.
- 1 of the 37 respondents confirmed that they require SOW to be established for higher risk customers only.
- 10 of the 37 respondents confirmed that the requirement for SOW to be established is applied and collected at the firm's discretion.



- 3 of the 37 respondents confirmed the establishment of a customer's SOW is never collected.

In line with paragraphs 14(3) and 15(3)(c) of the Code, as a minimum, relevant persons are required to take

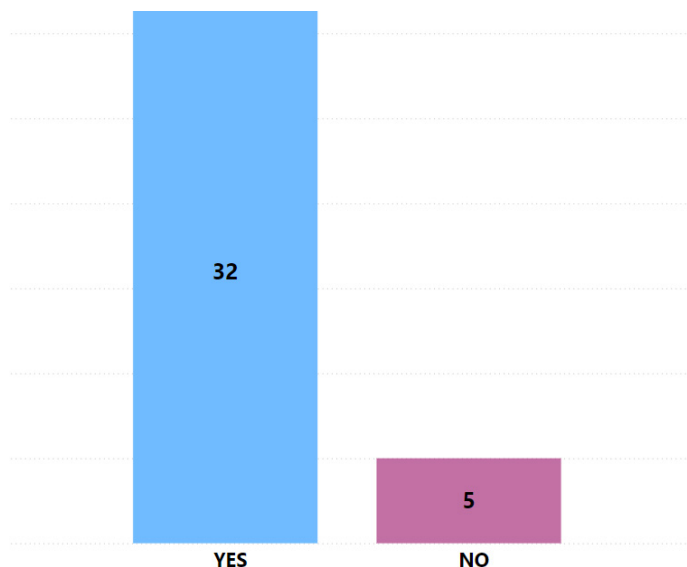
reasonable measures to establish a customer's SOW for any higher risk customers (including higher risk domestic PEPs), for all foreign PEPs, in the event of any unusual activity, and in the event of any suspicious activity (unless doing so would tip off the customer).

Legal persons are required to take reasonable measures to establish a customer's Source of Wealth for any higher risk customers

Q52: Where applicable, are reasonable measures taken to verify the SOW information collected?

32 respondents answered “Yes” advising that they take reasonable measures to verify the SOW information collected for a customer where applicable, and 5 respondents answered “No” advising that they do not do this.

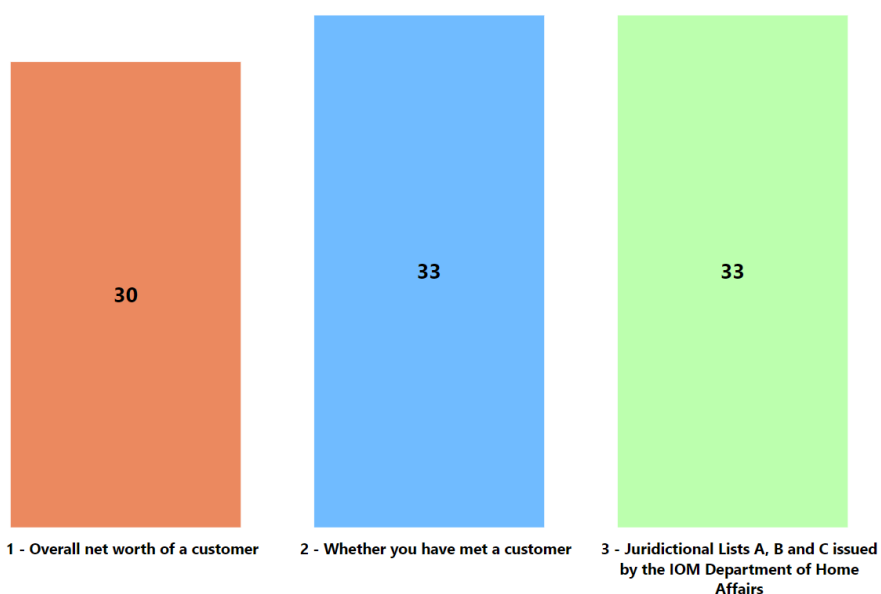
Further detail around SOW and the verification of SOW information can be found at sections 3.8.5, 3.8.6 and 3.8.7 of the Handbook.



Q53-55: Do you consider when assessing the risk of a customer relationship:

- The overall net worth of a customer;
- Whether you have met a customer; and
- Jurisdictional Lists A, B and C issued by the Isle of Man Department of Home Affairs.

Paragraphs 15(5) and 15(7) of the Code lay out matters that pose a higher risk of ML/FT and matters that may pose a higher risk of ML/FT.



Q53-55 asked Moneylenders whether they consider a number of these factors when assessing the risk of a customer relationship.

30 of the 37 respondents confirmed

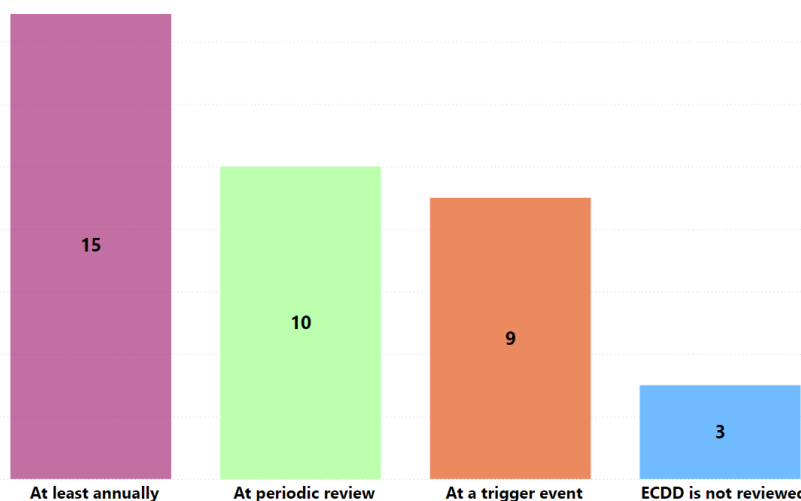
that they consider the overall net worth of a customer when assessing the risk of a customer relationship.

33 of the 37 respondents confirmed that they consider both whether

they have met a customer, and the jurisdictional Lists A, B and C issued by the Isle of Man Department of Home Affairs when assessing the risk of a customer relationship.

Q57: How often is ECDD reviewed?

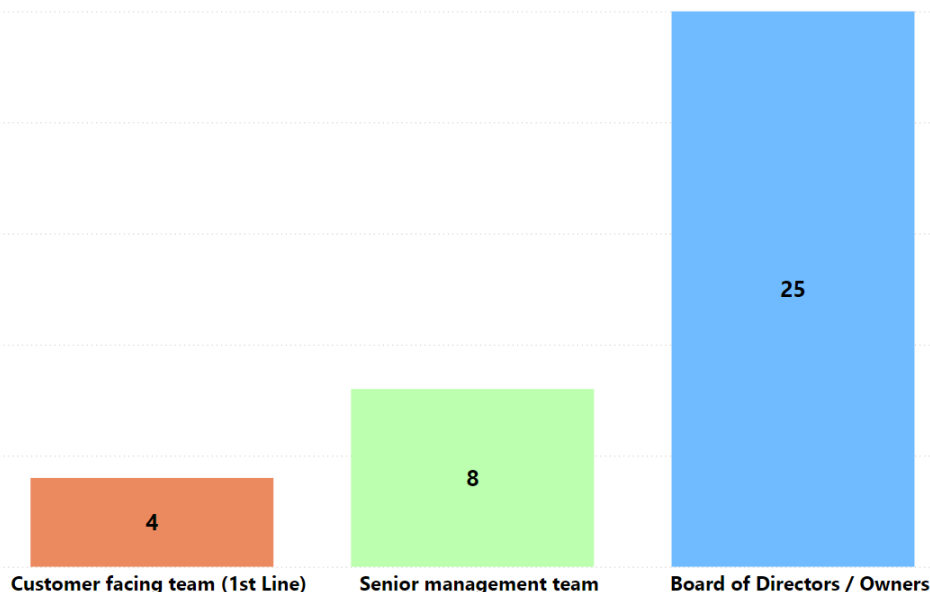
When answering the question how often is ECDD reviewed, the most common answer by respondents was at least annually, with 15 of the 37 Moneylenders providing this answer. 10 respondents stated that ECDD is reviewed at periodic review and 9 respondents stated that ECDD is reviewed at a trigger event. Only 3 of the 37 respondents stated that ECDD is not reviewed.



3.4 Onboarding and New Business Risks

Q58: Who is typically ultimately responsible for approving any new business for non-higher risk or non-PEP customers?

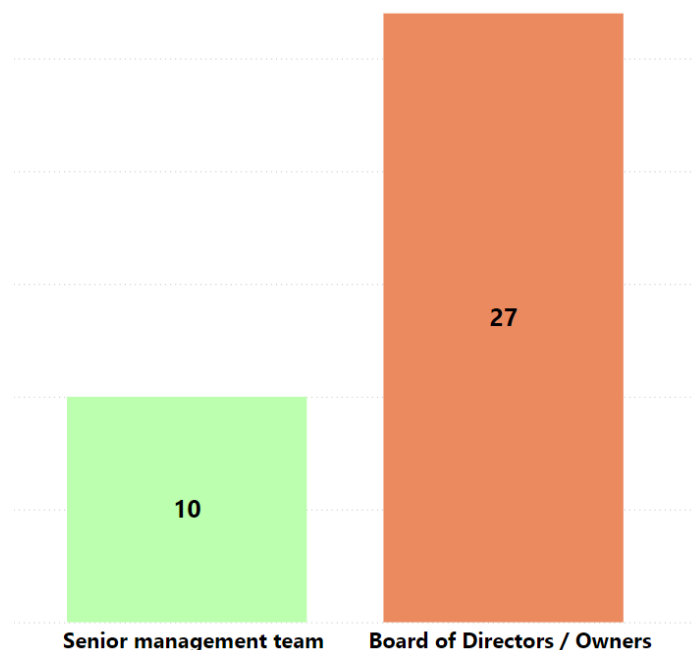
Most Moneylenders place the responsibility for approving new business for non-higher risk or non-PEP customers with the board of directors/owners, with 25 respondents providing this answer. A small proportion, 8 respondents, answered that this responsibility lies with the senior management team. Only 4 respondents stated that the customer facing team are responsible for approving new business for non-higher risk or non-PEP customers.



Q59: Who is typically ultimately responsible for approving any new business for higher risk or PEP customers?

In total 27 of the 37 respondents place the responsibility for approving new business for higher risk or PEP customers with the board of directors/owners. The remaining 10 respondents advised that they place this responsibility with the senior management team.

As required by paragraph 14(2) of the Code, senior management approval is required before the establishment of a business relationship, an occasional transaction being carried out or any business relationship being continued with a higher risk domestic PEP or any foreign PEP. Additionally, paragraph 15(6) of the Code lays out further circumstances whereby a relevant person's senior management must approve the establishment or continuation of a business relationship or occasional transaction.



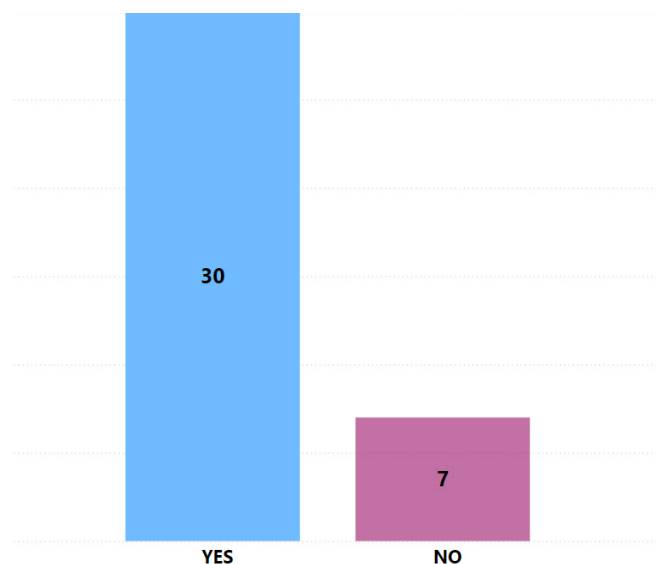
3.5 Natural Persons

Q60: Would you/do you lend to natural persons?

In total 30 of the 37 respondents advised that they would/do provide lending services to natural persons.

The Handbook outlines at section 3.5.1:

“When dealing with natural persons the identity is the specification of a unique natural person that is based on characteristics of the person that establish a person’s uniqueness in the population or particular context; and is recognised by the state for official purposes.”



Q61-67: Photo identification documents accepted by firms for natural persons:

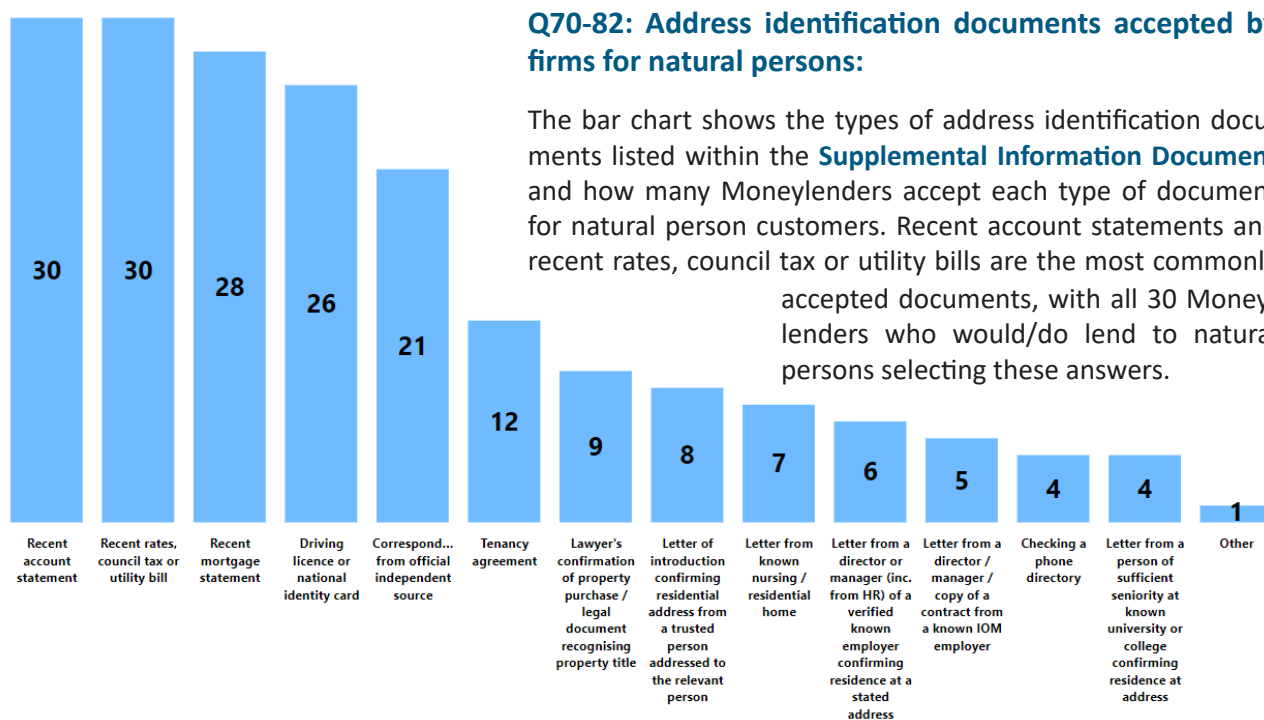
The bar chart provides an overview of the types of photo identification documents taken from the **Supplemental Information Document** which are accepted by respondents for natural person customers.

Passports and driving licenses proved to be the most commonly accepted forms amongst the respondents, with all 30 Moneylenders who would/do lend to natural persons selecting these answers.



Q70-82: Address identification documents accepted by firms for natural persons:

The bar chart shows the types of address identification documents listed within the **Supplemental Information Document** and how many Moneylenders accept each type of document for natural person customers. Recent account statements and recent rates, council tax or utility bills are the most commonly accepted documents, with all 30 Moneylenders who would/do lend to natural persons selecting these answers.

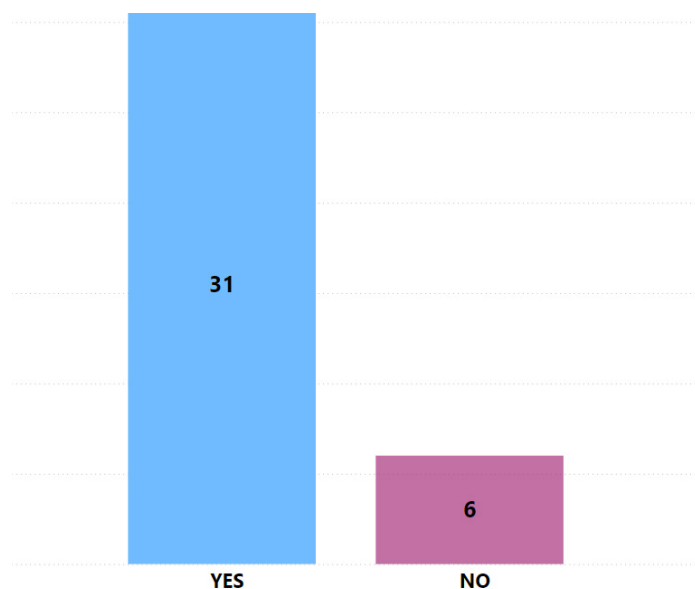


3.6 Legal Persons

Q92: Would you/do you lend to a legal person?

In total, 31 out of the 37 Moneylenders confirmed that they would/do lend to legal persons.

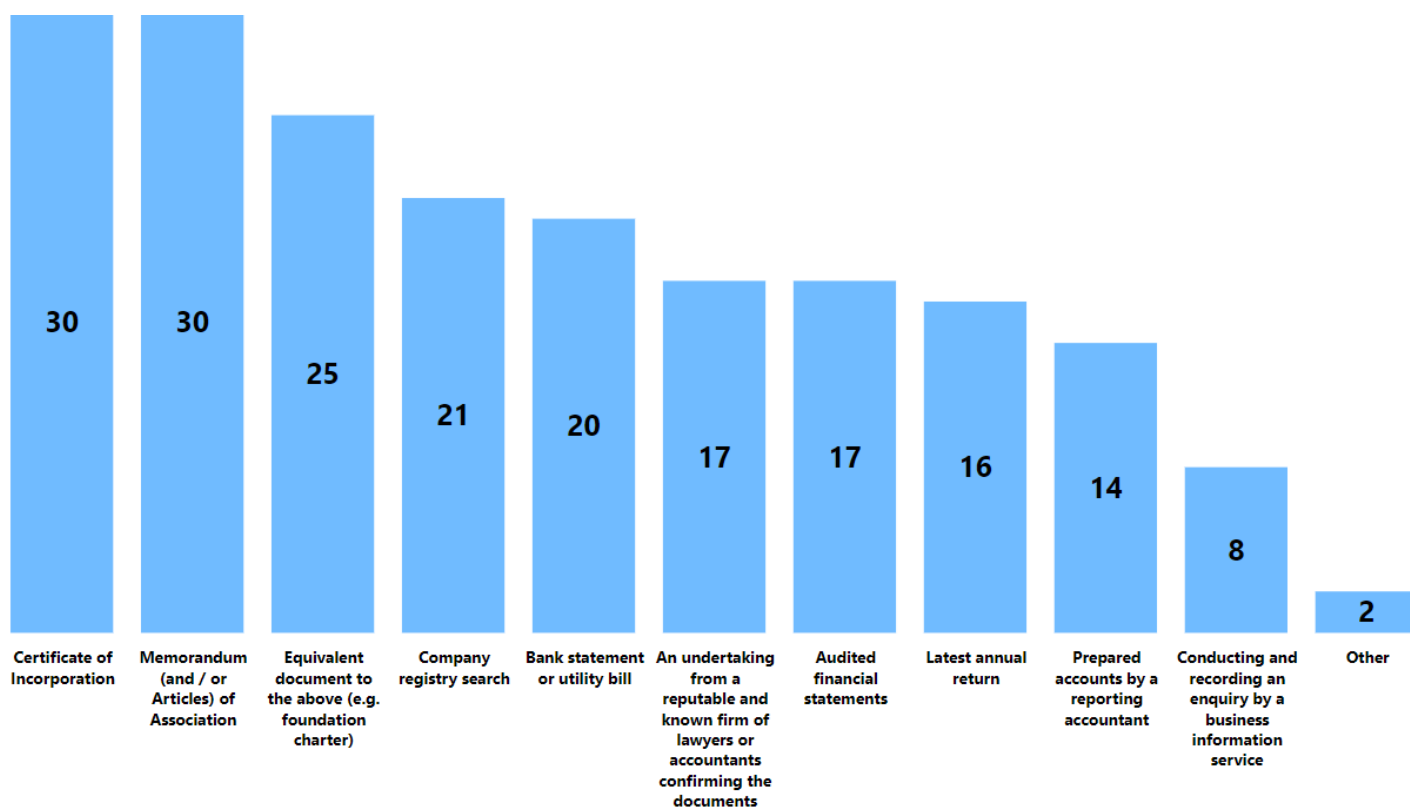
A legal person is defined in the Code as “any body corporate or unincorporate capable of establishing a business relationship with a relevant person or of owning property”.



Q93-102: Identification documents accepted by firms for legal persons:

The chart below provides an overview of the identification documents listed in the [Supplemental Information](#)

Document which are accepted by firms for legal persons. This shows certificates of Incorporation and Memorandum (and/or Articles) of Association as the most common forms.



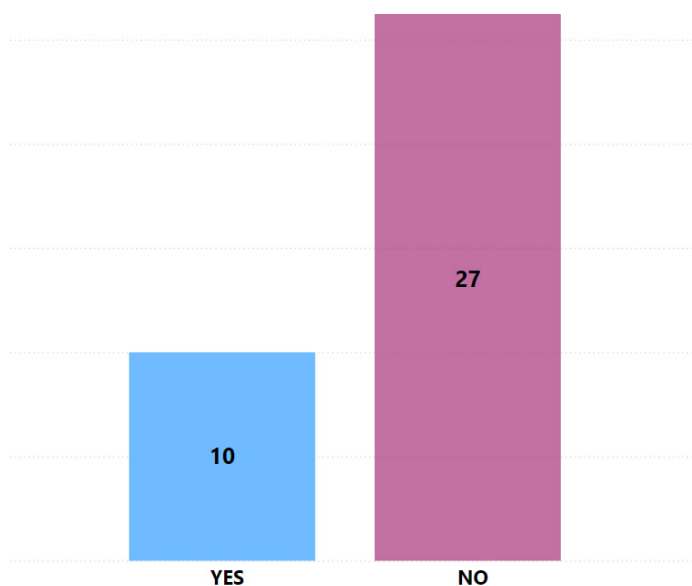
Legal person: ‘Any body corporate or unincorporate capable of establishing a business relationship with a relevant person or of owning property.’

3.7 Legal Arrangements

Q105: Would you/do you lend to a legal arrangement (e.g. a trust)?

In total only 10 of the 37 respondents advised that they would/do offer lending services to a legal arrangement.

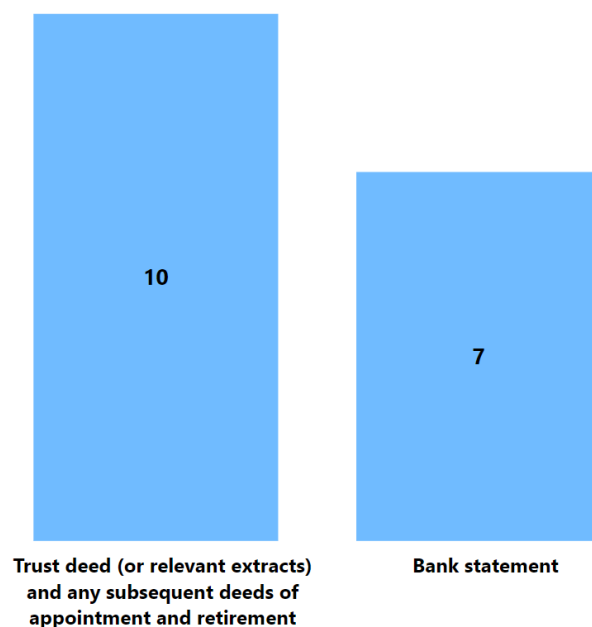
A legal arrangement is defined by the Code as including an express trust or any other arrangement that has a similar legal effect (including a fiducie, treuhand or fideicomiso) and includes a person acting for, or on behalf of, a legal arrangement such as a trustee.



Q106-107: Identification documents accepted by firms for legal arrangements:

The bar chart shows the breakdown of types of identification documents listed in the Supplemental Information Document which are accepted by firms in respect of legal arrangements. Trust deeds/subsequent deeds of appointment and retirement are the most utilised, with all 10 respondents who would/do lend to a legal arrangement selecting this answer.

7 of the 10 respondents who would/do lend to a legal arrangement confirmed they would accept a bank statement as identification for a legal arrangement.

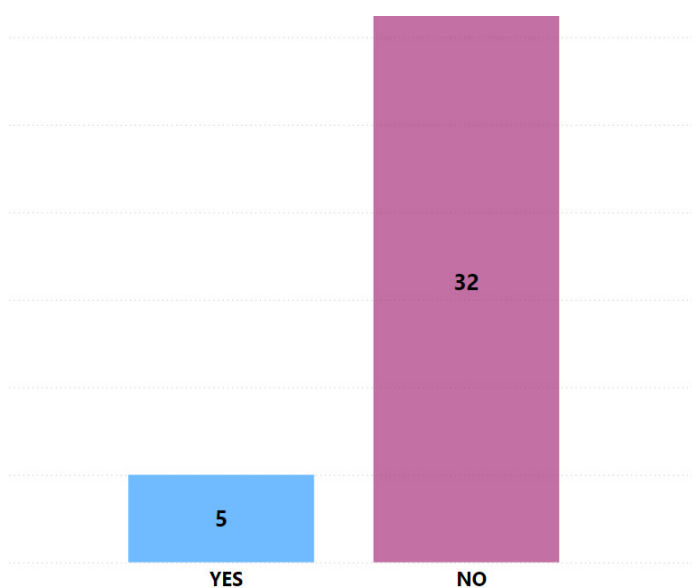


3.8 Foundations

Q110: Would you/do you lend to a foundation?

The responses show that the majority of respondents do not lend to foundations, with only 5 answering “Yes” that they do/would lend to a foundation.

A foundation is defined in the Code as meaning “a foundation established under the Foundations Act 2011 or a foundation or similar entity established under the law of another jurisdiction”.

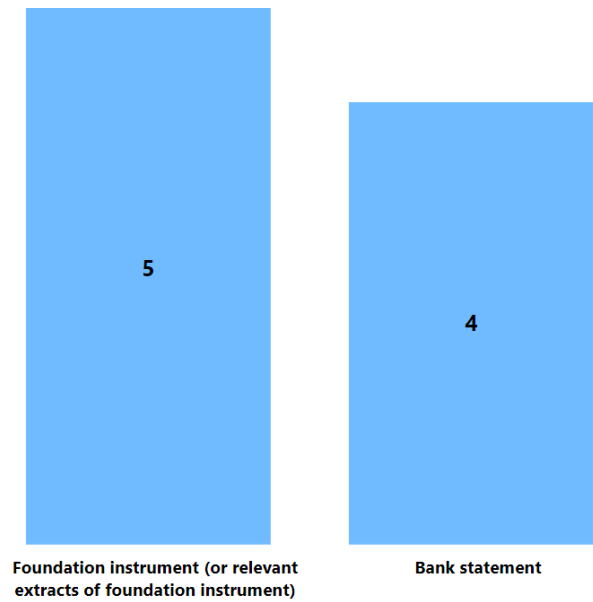


Q111-112: Identification documents accepted by firms for a foundation:

The bar chart shows the types of identification documents listed in the Supplemental Information Document which are accepted by firms for a foundation.

All 5 Moneylenders who confirmed they would/do lend to a foundation advised they would accept a copy of the foundation instrument as an identification document for the foundation.

4 Moneylenders confirmed they would accept a bank statement as an identification document for the foundation.



3.9 Electronic Methods

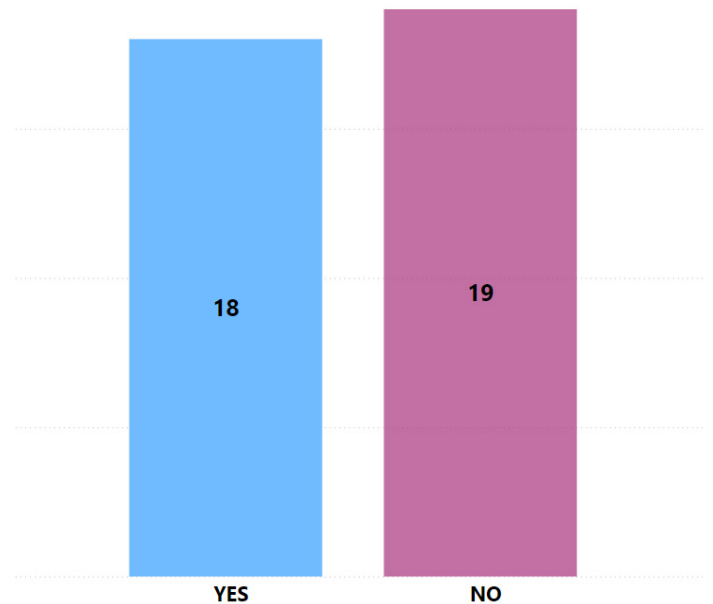
Q85: Would you/do you use electronic methods to verify identity and address?

18 of the 37 respondents answered “Yes”, confirming that they would/do use electronic methods to verify identity and address. 19 respondents answered “No”.

The Code and Handbook are technology neutral and so relevant persons may choose to use technology to meet their CDD obligations.

The Handbook states that:

“Relevant persons should understand the basis for any electronic method, and be satisfied that it is sufficiently robust. This includes knowing what checks have been undertaken and the results of those checks. Relevant persons should also understand the method(s) used for corroboration of identity data and the potential for processes to be abused. Relevant persons must ensure that whatever electronic methods are used, they are capable of being monitored

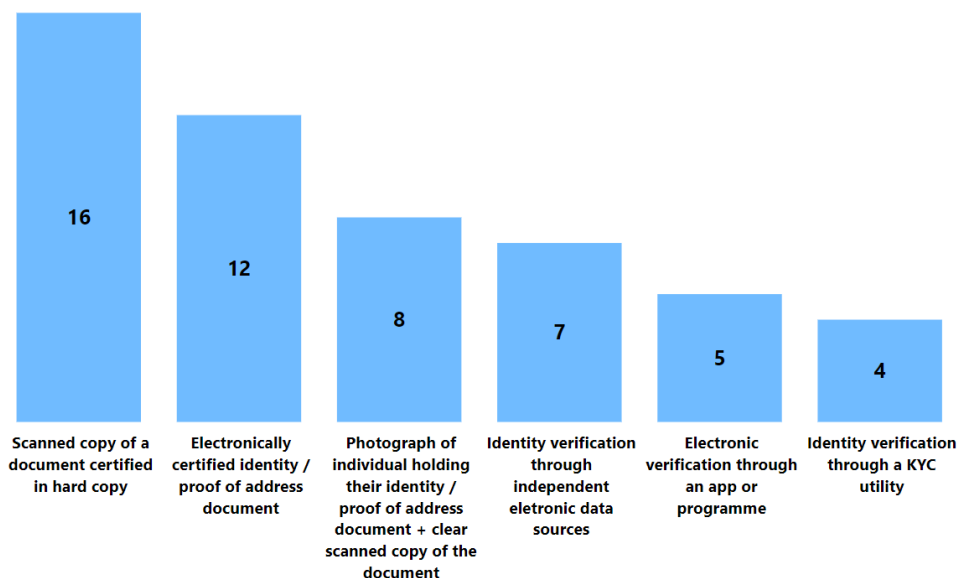


and tested to ensure they enable the relevant persons to meet their AML/CFT obligations as anticipated and continue to do so.”



Q86-91: Electronic methods to verify identity and address used by firms:

The bar chart outlines the electronic methods listed in the **Supplemental Information Document** used by firms to verify identity and address.

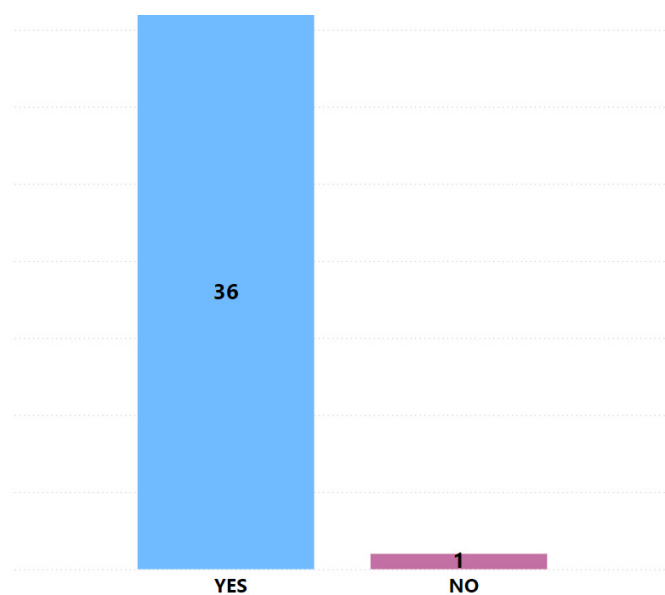


3.10 Controls

C1: Do you have documented AML/CFT procedures and controls in place?

36 of the 37 respondents confirmed that documented AML/CFT procedures and controls are in place. It has subsequently been identified that the 1 “No” answer provided to this question was made in error⁵.

Paragraph 4 of the Code requires the relevant person to have in place procedures prior to entering into a business relationship or occasional transaction.

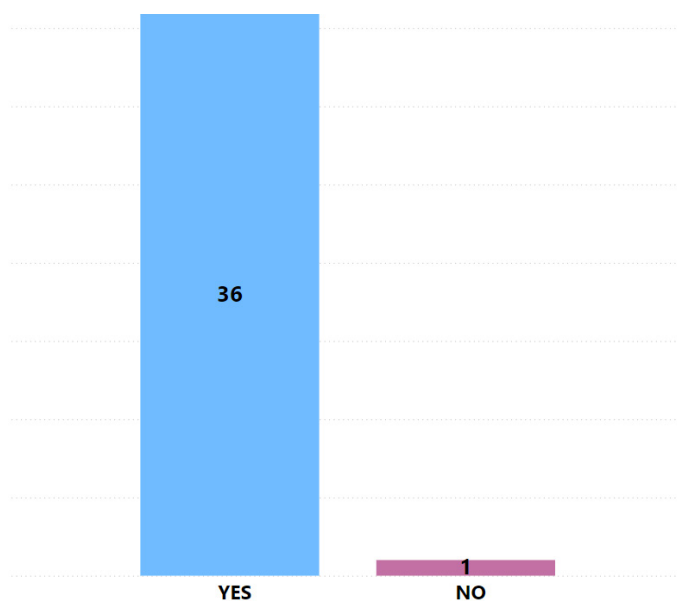


C2: Are employees aware of the AML/CFT procedures and controls established?

36 of the 37 respondents confirmed that their employees are aware of the procedures and controls in place. Similarly to C1, it has been identified the 1 “No” answer to this question was made in error⁵.

The Handbook sets out that procedures and controls must be established in writing, must be understandable and appropriately accessible to all those involved in the business.

Procedures and controls must be operated consistently and where deviations are made there should be documented approval in place to evidence consideration of ML/TF risks and how they can be managed.

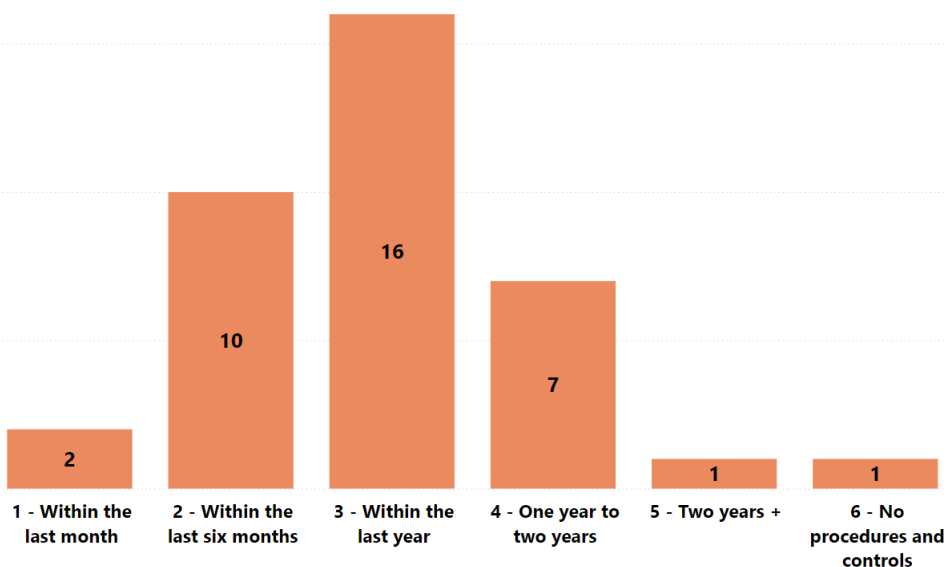


⁵ Due to this reporting error, answers to questions C1 to C4, C6 and C7 may not be truly representative of the sector.

C3: When were these AML/CFT procedures last updated?

The below bar chart illustrates when firms' AML/CFT procedures were last updated.

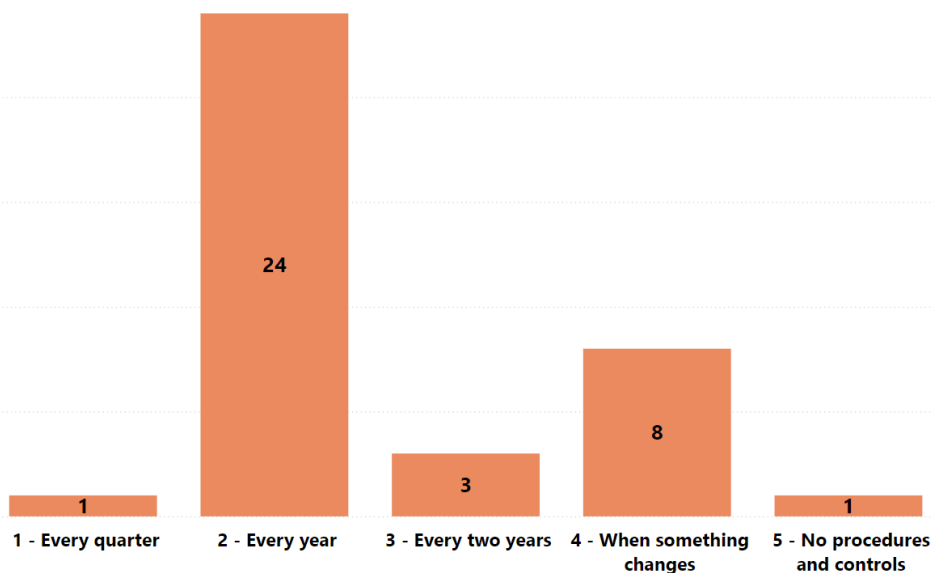
"Within the last year" was the most prevalent response with 16 respondents selecting this answer out of the 37 total.



C4: How often are these AML/CFT procedures typically reviewed?

24 of the 37 respondents typically review the procedures and controls every year.

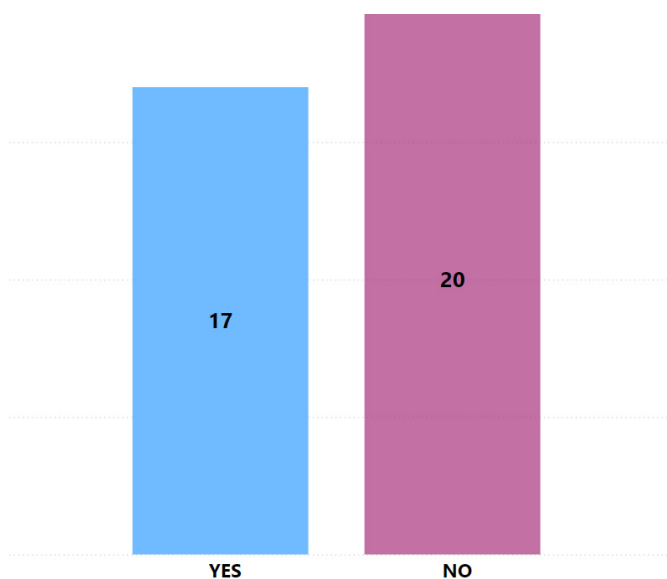
Paragraph 4(1)(a) of the Code requires a firm's procedures and controls to be maintained and it is important to ensure that they remain fit for purpose.



C5: Do you have documented procedures and controls in place to deal with deviations from your CDD and ECDD process?

In response to this question the responses were fairly evenly split between "Yes" deviations are documented and "No" that they are not.

It is important that any deviations, from CDD/EDD procedures and any others, are formally documented to ensure that there is a record of ML/TF risk considerations and mitigation. The deviation, assessment, rationale and approval should be fully documented.

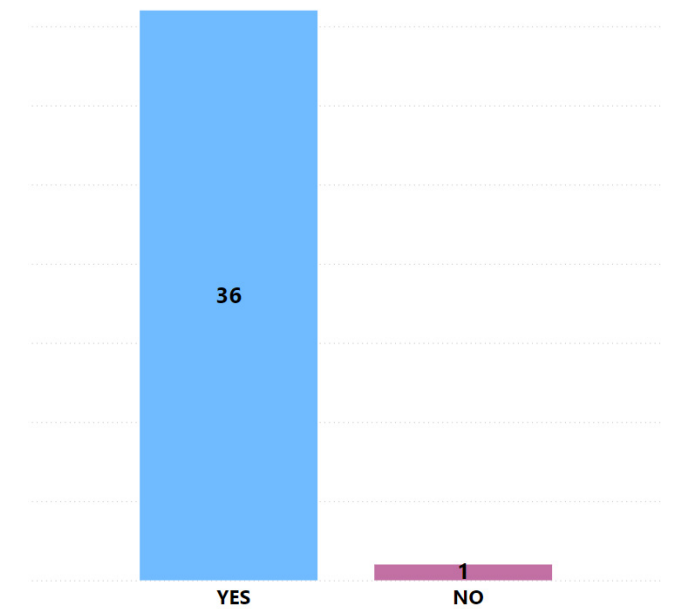


C6: Do you have documented procedures and controls in place specifically relating to the collection of CDD?

The majority of respondents, 36 out of the 37 Moneylenders, answered “Yes” confirming that they have documented procedures and controls in place specifically relating to the collection of CDD. It has subsequently been identified that the 1 “No” answer provided to this question was made in error.

Robust CDD procedures ensure that relevant persons are aware of the potential ML/TF risks posed by their customers during the course of the business relationship.

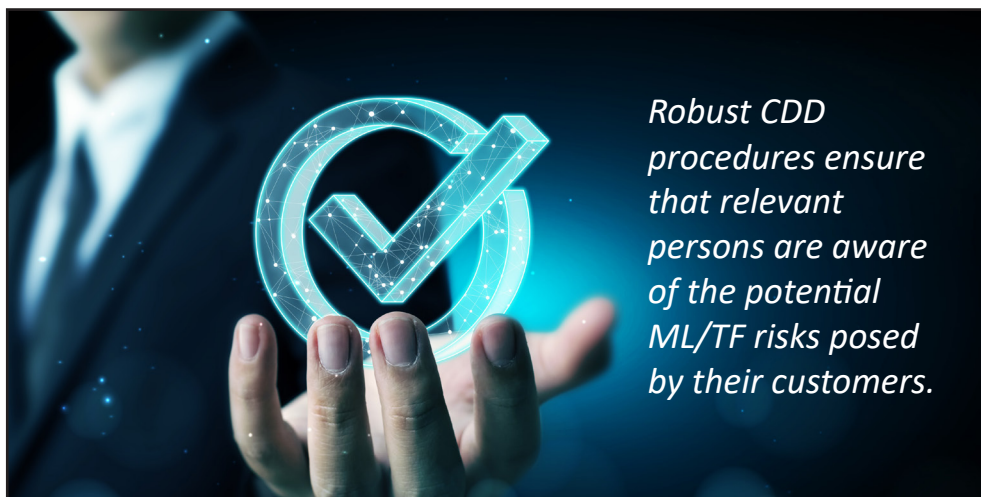
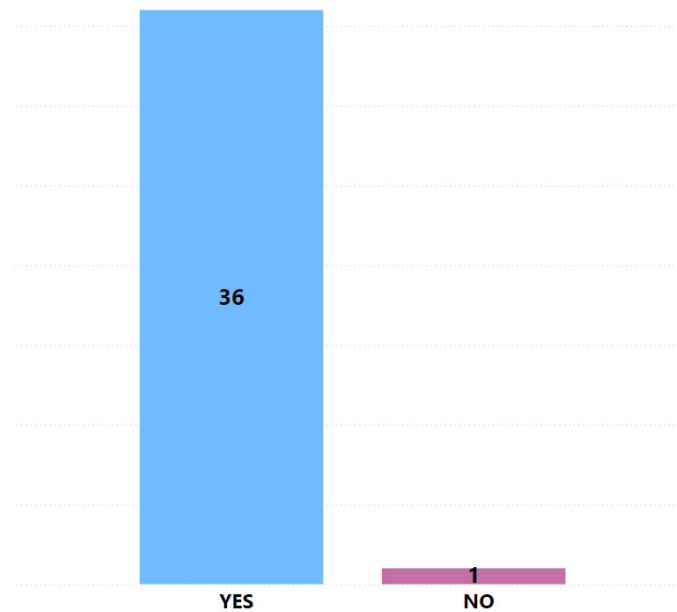
The procedures are vital to forestalling abuse of the financial system by criminals or those seeking to use it for terrorism purposes. CDD is integral to managing and mitigating ML/TF risks, and without satisfactory CDD, effective risk assessments and ongoing monitoring for suspicious or unusual activity is not possible.



C7: Do these procedures and controls include a list of source documents, data and information that the firm is willing to accept as CDD?

All respondents who confirmed that they have documented procedures and controls in place specifically relating to conducting CDD, also confirmed that these procedures and controls include a list of source documents, data and information that the firm is willing to accept as CDD, with 36 respondents answering “Yes” to this question. It has subsequently been identified that the 1 “No” answer provided to this question was made in error.

Only 1 respondent answered “No” to this question which was the same firm who answered “No” to the previous question.

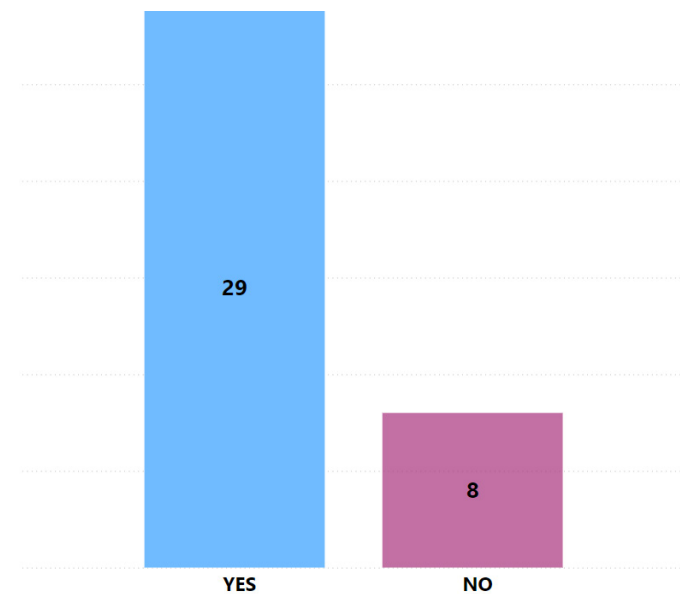


C8: Do you have documented procedures and controls in place specifically relating to the collection of ECDD?

In total, 29 of the 37 respondents answered “Yes” to this question advising that they have documented procedures and controls in place specifically relating to conducting ECDD, whilst 8 respondents answered “No” meaning they do not have such procedures and controls in place.

In line with paragraph 4 of the Code, firms must establish, record, operate and maintain procedures and controls in order to comply with each paragraph within Parts 3 to 9 of the Code. This includes paragraph 15 of the Code which details the requirements for ECDD.

Even if a firm does not have any customers they are required to/consider it necessary to conduct ECDD on, procedures and controls should still be in place to address this and outline when ECDD would be required/considered

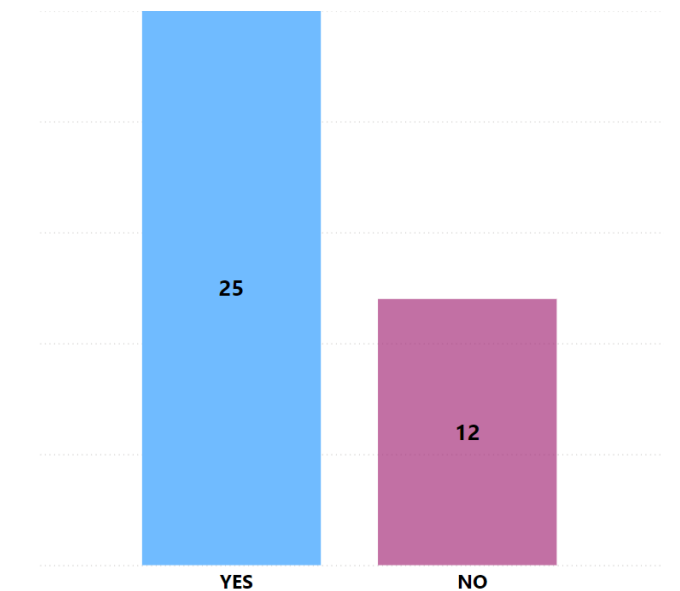


necessary, as circumstances may arise during established business relationships where ECDD must be carried out.

C9: Do these procedures and controls include a list of source documents, data and information that the firm is willing to accept as ECDD?

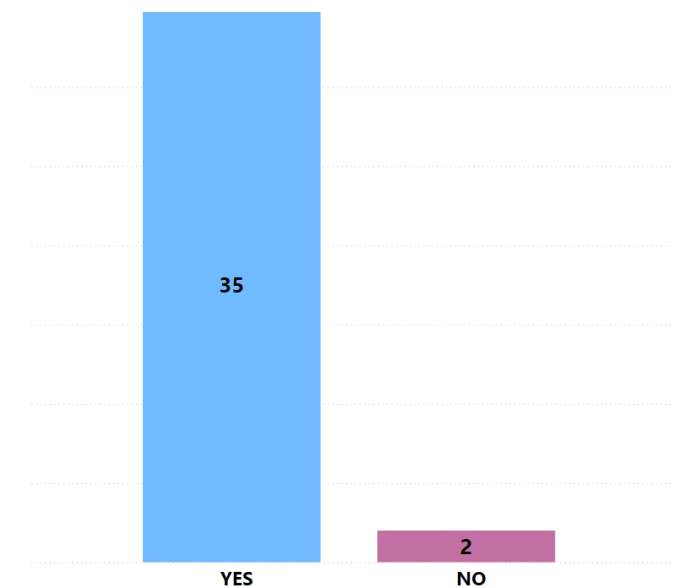
Out of the 29 respondents who answered “Yes” to the previous question, 25 of these respondents confirmed that their documented ECDD procedures and controls include a list of source documents, data and information that the firm is willing to accept as ECDD by answering “Yes” to this question.

A total of 12 respondents answered “No” to this question, which includes the 8 respondents who confirmed in the previous question that they do not have documented procedures and controls in place specifically relating to conducting ECDD.



C10: Do your procedures and controls cover acceptable methods of verification of CDD and ECDD information (e.g. independent certification or electronic verification)?

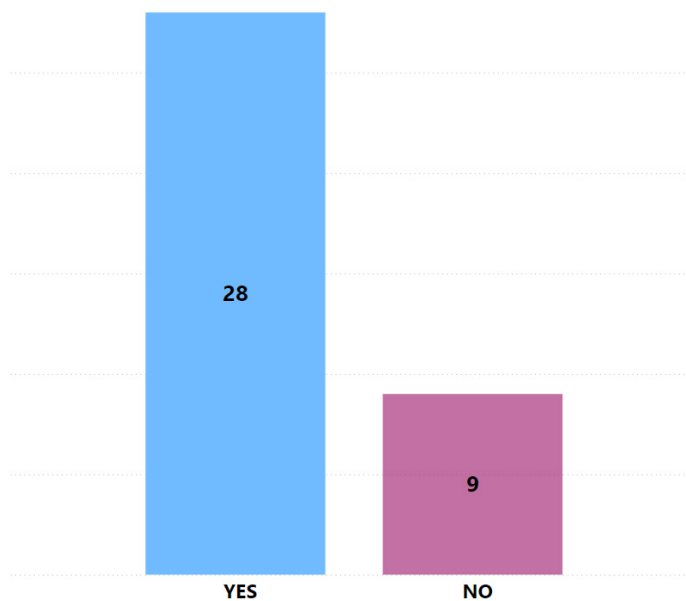
35 respondents answered “Yes” to this question, confirming that their procedures and controls cover acceptable methods of verification of CDD and ECDD. Only 2 respondents answered “No” advising that they do not have such procedures and controls in place.



C11: Do you have procedures and controls in place regarding electronic methods of receiving/verifying CDD and/or ECDD?

28 of the 37 respondents answered “Yes” to this question confirming that they have procedures and controls in place regarding electronic methods of receiving/verifying CDD and/or ECDD. 9 respondents answered “No” confirming that they do not have such procedures and controls in place.

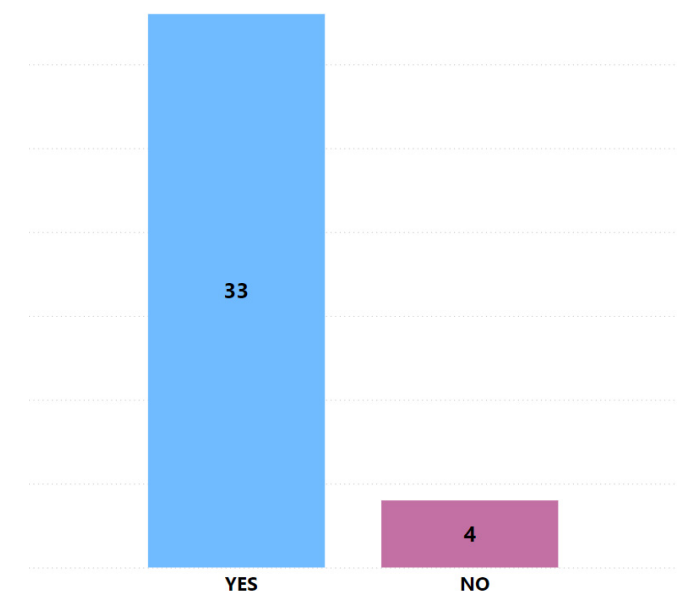
The Code and the Handbook remain technology neutral, so it is for a relevant person to decide whether they choose to use technology to meet their CDD/ECDD obligations. However, the Authority highlights that it is vital for relevant persons choosing to use technology to assist in meeting their CDD/ECDD obligations to establish effective procedures and controls relating to this.



C12: Do you have documented procedures and controls in place which meet the requirements of paragraphs 8(5) and 15(8) of the Code?

The majority of respondents, 33 of 37 Moneylenders, answered “Yes” to this question, advising that they have documented procedures and controls in place which meet the requirements of paragraphs 8(5) and 15(8) of the Code. Only 4 respondents answered “No” to this question.

Paragraphs 8(5) and 15(8) of the Code outline what a relevant person’s procedures and controls must require where the requirements of paragraph 8/paragraph 15 of the Code are not met. It is therefore essential that relevant person’s procedures and controls clearly address these circumstances.

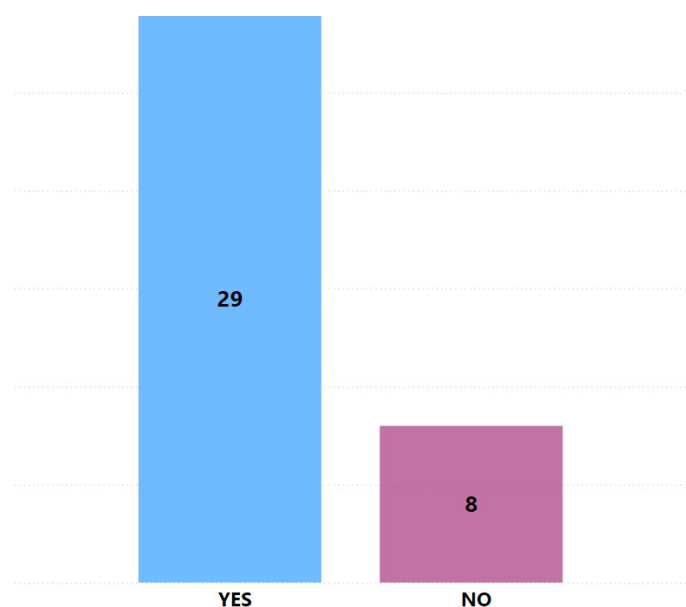


C13: Do you have documented procedures and controls in place specifically relating to SOF?

29 of the 37 respondents confirmed that they have documented procedures and controls in place specifically relating to SOF by answering “Yes” to this question, whilst 8 respondents answered “No”.

Paragraph 8(3)(e) of the Code requires a relevant person to establish, record, maintain and operate procedures and controls in relation to taking reasonable measures to establish a customer’s SOF.

Relevant persons should remember that SOF is a twofold concept made up of both the origin of the particular funds or other assets involved in a business relationship or occasional transaction (including the activity that generated these funds), and also the means through which the funds were transferred.

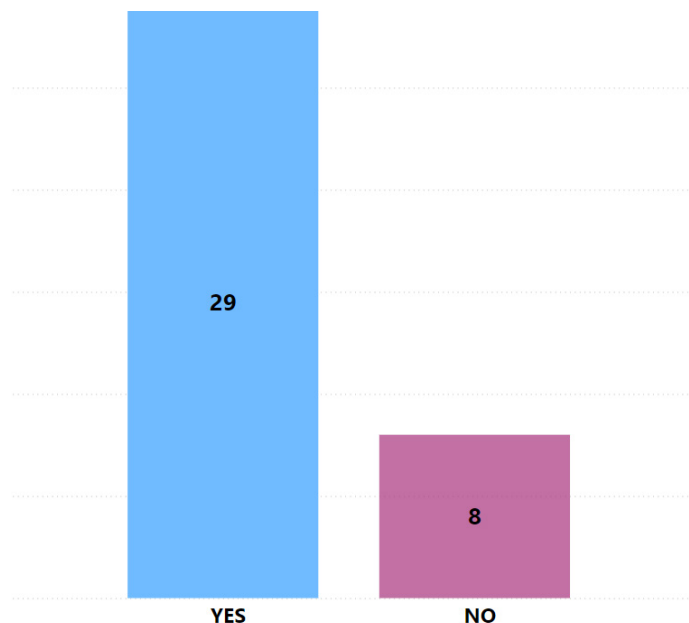


C14: Do you have documented procedures and controls in place specifically relating to SOW?

29 of the 37 respondents confirmed that they have documented procedures and controls in place specifically relating to SOW. These were the same 29 respondents who answered “Yes” to the previous question. Similarly, 8 respondents answered “No”.

The minimum requirements laid out in the Code are that reasonable measures to establish SOW are required for higher risk customers (including higher risk domestic PEPs), foreign PEPs, in the event of any unusual activity, and in the event of any suspicious activity (unless the relevant person believes this will tip off the customer).

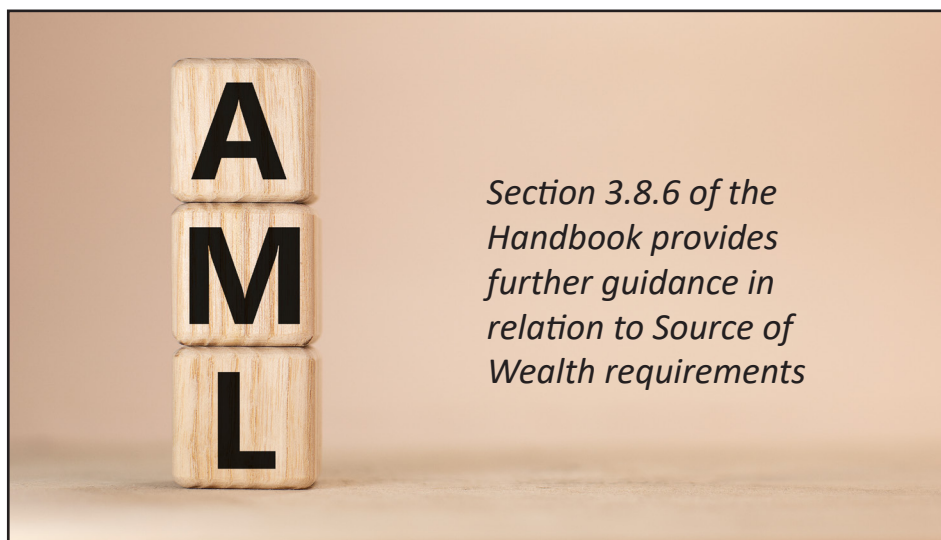
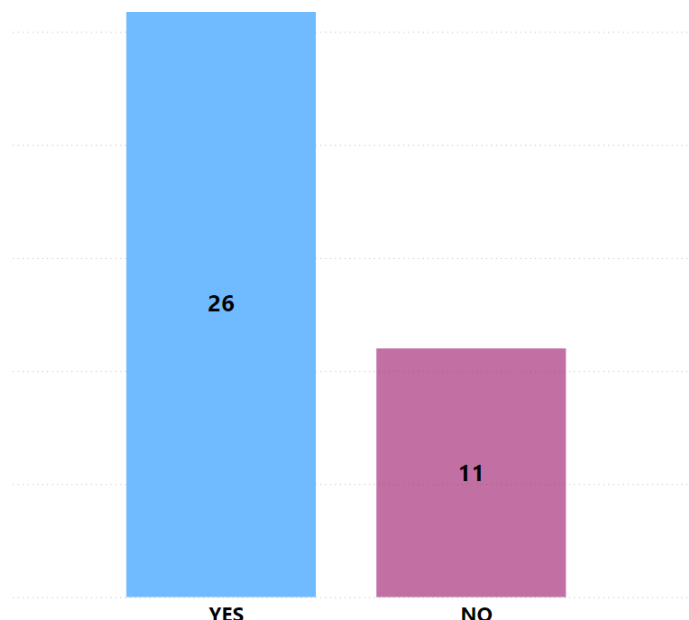
Section 3.8.6 of the Handbook provides further guidance, stating that “Source of wealth requirements are risk based and the procedures and practices put in place to satisfy the requirements must enable relevant persons to manage and mitigate their identified ML/FT risks.”



C15: Do procedures and controls include the firm’s approach to SOF and SOW, including what information/documentation should be collected?

Of the 29 respondents who confirmed they have documented procedures and controls in place specifically relating to SOF and SOW, 26 of these advised that the procedures and controls include the firm’s approach to SOF and SOW, including what information/documentation should be collected by answering “Yes” to this question.

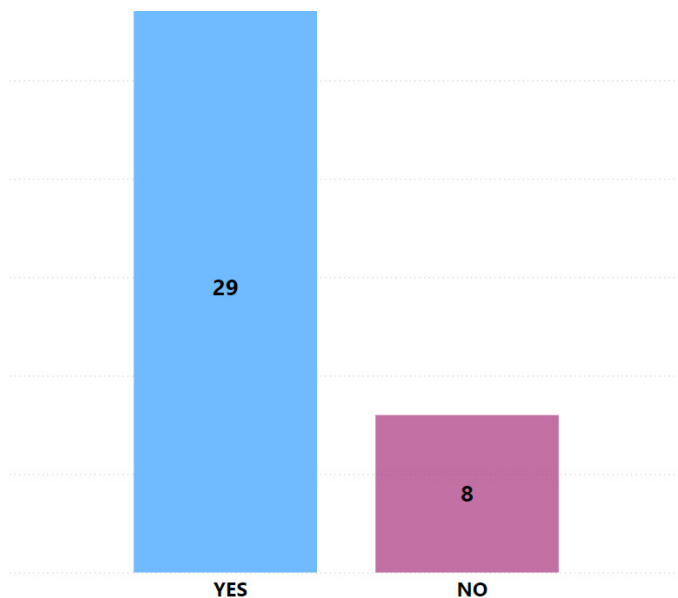
11 of the 37 respondents answered “No”, confirming that their procedures and controls do not include this information. Sections 3.8 of the Handbook contains detailed guidance on SOF and SOW, including examples of SOF and SOW and examples of information which may be collected to verify the accuracy of a customer’s declaration about their SOF or SOW.



C16: Do procedures and controls include when SOF and SOW should be collected?

All 29 respondents who confirmed they have documented procedures and controls in place specifically relating to SOF and SOW also confirmed that these procedures and controls include when SOF and SOW should be collected.

As previously highlighted within this report, the minimum requirements required by the Code are reasonable measures to establish SOF for all new business relationships in line with paragraph 8(3)(e) of the Code, and reasonable measures to establish SOW for all higher risk customers (including higher risk domestic PEPs), all foreign PEPs, in the event of any unusual activity, and in the event of any suspicious activity, in line with paragraphs 14 and 15 of the Code.

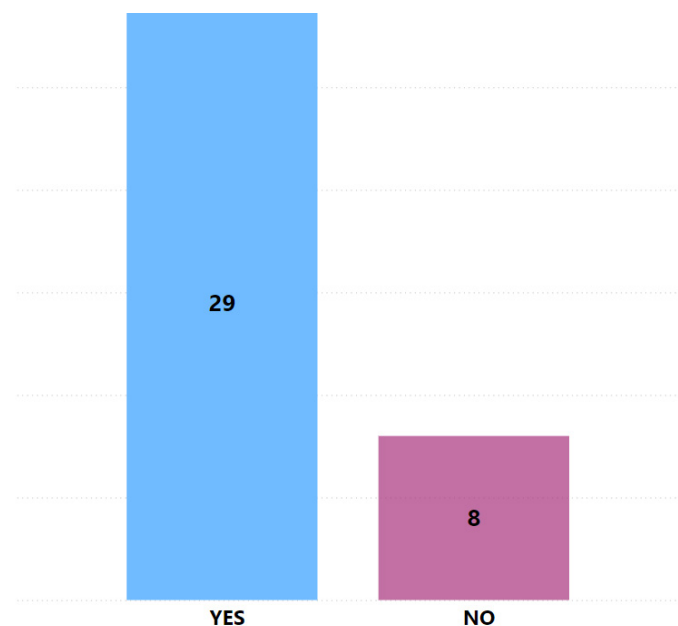


C17: Do procedures and controls consider SOF and SOW as separate concepts and include what the difference between SOF and SOW is?

All 29 respondents who confirmed they have documented procedures and controls in place specifically relating to SOF and SOW also answered “Yes” to this question, confirming that these procedures and controls consider SOF and SOW as separate concepts and include what the difference is between SOF and SOW.

“Funds” and “wealth” are two different concepts in the Code. As stated at section 3.8.5 of the Handbook, “source of wealth is distinct from source of funds and includes the customer’s funds that may never have anything to do with the relevant person.”

Whereas SOF are “the amounts being invested, deposited or wired as part of the business relationship/occasional transaction, both at the outset of the relationship and during its course”, as described at section 3.8.1 of the Handbook.



Appendix 1

Paragraph 8 of the Code

(8) New business relationships

(1) A relevant person must, in relation to each new business relationship, establish, record, maintain and operate the procedures and controls specified in sub-paragraph (3)

(2) Subject to sub-paragraph (4), the procedures and controls must be undertaken –

(a) before a business relationship is entered into; or

(b) during the formation of that relationship.

(3) Those procedures and controls are –

(a) identifying the customer;

(b) verifying the identity of the customer using reliable, independent source documents, data or information;

(c) verifying the legal status of the customer using reliable, independent source documents, data or information;

(d) obtaining information on the nature and intended purpose of the business relationship; and

(e) taking reasonable measures to establish the source of funds including where the funds are received from an account not in the name of the customer –

(i) understanding and recording the reasons for this;

(ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and

(iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements of paragraph 15.

(4) In exceptional circumstances the verification of the identity of the customer in accordance with sub-paragraphs (3) (b) and (c) may be undertaken after the formation of the business relationship if –

(a) it occurs as soon as reasonably practicable;

(b) the delay is essential so as not to interrupt the normal course of business;

(c) the customer has not been identified as posing a higher risk of ML/FT;

(d) the risks of ML/FT are effectively managed; and

(e) the relevant person has not identified any unusual activity or suspicious activity;

(f) the relevant person's senior management has approved the establishment of the business relationship and any subsequent activity until sub-paragraphs (3)(b) and (c) has been complied with; and

(g) the relevant person ensures that the amount, type and number of transactions is appropriately limited and monitored.

(5) Except as provided in sub-paragraph (4) and Part 6, where the requirements of this paragraph are not met, the procedures and controls must provide that –

(a) it occurs as soon as reasonably practicable;

(b) the delay is essential so as not to interrupt the normal course of business;

(c) the customer has not been identified as posing a higher risk of ML/FT;

(d) the risks of ML/FT are effectively managed; and

(e) the relevant person has not identified any unusual activity or suspicious activity;

(f) the relevant person's senior management has approved the establishment of the business relationship and any subsequent activity until sub paragraphs (3)(b) and (c) has been complied with; and

(g) the relevant person ensures that the amount, type and number of transactions is appropriately limited and monitored.

Paragraph 15 of the Code

(15) Enhanced customer due diligence

(1) A relevant person must establish, record, maintain and operate appropriate procedures and controls in relation to undertaking enhanced customer due diligence.

(2) Enhanced customer due diligence includes —

(a) considering whether additional identification information needs to be obtained and, if so, obtaining such additional information;

(b) considering whether additional aspects of the identity of the customer need to be verified by reliable independent source documents, data or information and, if so, taking reasonable measures to obtain such additional verification;

(c) taking reasonable measures to establish the source of the wealth of a customer;

(d) undertaking further research, where considered necessary, in order to understand the background of a customer and the customer's business; and

(e) considering what additional ongoing monitoring should be carried out in accordance with paragraph 13 and carrying it out.

(3) A relevant person must conduct enhanced customer due diligence —

(a) where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment;

(b) without limiting paragraph 13, in the event of any unusual activity; and

(c) without limiting paragraph 26, in the event of any suspicious activity, unless the relevant person reasonably believes conducting enhanced customer due diligence will tip off the customer.

(4) For the avoidance of doubt, if higher risk of ML/FT within the meaning of sub-paragraph (3)(a) is assessed, then paragraphs 8(4), 11(4), 11(5), 16 to 19, 20(2), (3), (5) and 21 do not apply.

(5) Matters that pose a higher risk of ML/FT include —

(a) a business relationship or occasional transaction with a customer that is resident or located in a jurisdiction in List A; and

(b) a customer that is the subject of a warning in

relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction.

(6) If sub-paragraph (5)(a) or (b) applies, the relevant person's senior management must approve the establishment, or continuation, of the business relationship or the occasional transaction.

(7) Matters that may pose a higher risk of ML/FT include —

(a) activity in a jurisdiction the relevant person deems to be higher risk of ML/FT;

(b) a business relationship or occasional transaction with a customer resident or located in a jurisdiction in List B;

(c) activity in a jurisdiction in List A or B;

(d) a situation that by its nature presents an increased risk of ML/FT;

(e) a business relationship or occasional transaction with a PEP;

(f) a company that has nominee shareholders or shares in bearer form;

(g) the provision of high risk products;

(h) the provision of services to high-net-worth individuals;

(i) a legal arrangement;

(l) persons performing prominent functions for international organisations;

(k) circumstances in which the relevant persons and the customer have not met — (i) during the business relationship or during its formation; or (ii) in the course of an occasional transaction; and (l) if the beneficiary of a life assurance policy is a legal person or legal arrangement.

(8) Except as provided in Part 6, where the requirements of this paragraph are not met within a reasonable time-frame, the procedures and controls must provide that —

(a) the business relationship or occasional transaction must proceed no further;

(b) the relevant person must consider terminating that relationship; and

(c) the relevant person must consider making an internal disclosure.



**ISLE OF MAN
FINANCIAL SERVICES AUTHORITY**

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Our mailing address is:

PO Box 58

Douglas

Isle of Man

IM99 1DT

Email:

info@iomfsa.im