ALICO UK LIMITED

AML Policy Procedures and Program

383a Green Street London E13 9AU United Kingdom

383a Green Street
London E13 9AU
United Kingdom

Phone Number: 44 020 8470 9333
Email: alicoexchange@hotmail.com

July 2020

CONTENTS

EXECUTIVE SUMMARY **3**

INTRODUCTION: **4**

NOMINATED OFFICER (MONEY LAUNDERING REPORTING OFFICER) AND COMPLIANCE OFFICER **5**

CONTENTS OF THIS GUIDANCE **6**

COMPANY ANTI-MONEY LAUNDERING POLICY STATEMENT **7**

WHAT IS MONEY LAUNDERING AND WHAT THE UK LAW REQUIRES **8**

MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) REGULATIONS 2019 ..... **8**

PAYMENT SERVICE REGULATION 2017 ..... **10**

CRIMINAL FINANCES ACT 2017 ..... **11**

WHAT ARE THE OFFENCES AND PENALTIES? **13**

THE PROCEEDS OF CRIME ACT 2002 (POCA) AS AMENDED BY THE SERIOUS ORGANISED CRIME AND POLICE ACT 2005 ..... **13**

WHAT IS TERRORISM **14**

WHAT IS A DIRECTION ISSUED UNDER SCHEDULE 7 TO THE COUNTER-TERRORISM ACT 2008 (A 'DIRECTION')? **15**

COUNTER TERRORISM ACT 2008 SCHEDULE 7 ..... **15**

WHAT IS THE FINANCIAL ACTION TASK FORCE (FATF)? **16**

WHAT ARE SANCTIONS? **16**

BRIBERY OFFENCES AS PER BRIBERY ACT 2010 AND PENALTIES: **17**

PENALTIES **18**

KYC PROCESS AND CUSTOMER ONBOARDING / CUSTOMER DUE DILIGENCE (CDD) **18**

ONGOING MONITORING OF TRANSACTIONS **25**

OBTAINING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF A BUSINESS RELATIONSHIP: **27**

OCCASIONAL TRANSACTIONS **28**

ENHANCED DUE DILIGENCE (EDD) POLICY **28**

POLITICALLY EXPOSED PERSONS (PEPS) CHECK **29**

SANCTIONS LIST CHECK **30**

REPORTING SUSPICIOUS ACTIVITY 31
MAKING A SUSPICIOUS ACTIVITY REPORT TO NCA 32
STAFF AWARENESS AND TRAINING 34
RECORD KEEPING 36

EXECUTIVE SUMMARY

Our company is committed to complying with all legislation that is designed to combat money laundering and terrorist financing. This includes ensuring that we have adequate controls to counter money laundering and terrorist financing, as detailed in this document, and that we train staff appropriately.

Our risk assessment indicates that our company has a low risk of being used to launder money or to handle terrorist finances. Nevertheless, we keep our procedures under regular review and we monitor the transactions that we process in order to ensure that our procedures are being followed. We recognize the importance of staff promptly reporting suspicious activity. We have appointed a Nominated Officer (also known as a Money Laundering Reporting Officer or MLRO). We have in place appropriate procedures, which are detailed in this document, to obtain and verify evidence of the identity of our customers and to monitor ongoing activity.

Objectives

The purpose of this document is to provide detailed procedures to ensure we meet our legal obligations to deter detect and disrupt money laundering and terrorist financing. The document:

- Outlines the legislation on anti-money laundering (AML) and combating terrorist financing (CTF) measures;
- Explains the requirements of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 and how these should be applied in practice;
- Gives details of the systems and controls necessary to lower the risk of our company being used by criminals to launder money or finance terrorism.

What is money laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. It also covers money, however come by, which is used to fund terrorism.

- Money Laundering can take many forms including:
- Acquiring, using or possessing criminal property;
- Handling the proceeds of crimes such as theft, fraud and tax evasion;
- Being knowingly involved in any way with criminal or terrorist property;
- Entering into arrangements to facilitate laundering criminal or terrorist property;
- Investing the proceeds of crimes in other financial products;
- Investing the proceeds of crimes through the acquisition of property/assets;
- Transferring criminal property.

INTRODUCTION:

The purpose of this guide is to inform employees, senior management, UK MSB customers and foreign correspondents as to the Anti-Money Laundering (AML) and Counter Terrorist Finance (CTF) procedures that ***ALICO UK LIMITED*** has adopted and adheres to in its daily operations.

ALICO UK LIMITED provides (or is willing to) the following services to its customers:
Money remittance services

Money remittance services:

A money transfer service offered to a sending customer whereby a remittance payment is made to a named receiving customer, often in another country.

Thus, ***ALICO UK LIMITED*** is a Payment Institution and required by law to be regulated by the Financial Conduct Authority as well as HM Revenue & Customs.

Legislation:

The main UK legislation covering anti-money laundering and counter financing of terrorism is:

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- Criminal Finances Act 2017

The following legislation applies to money transmission businesses only:

- Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation)
- Payment Service Regulations 2017

Key facts about ALICO UK LIMITED

- A UK Registered Company with Head Office in London.
- Registered in companies house under **04402104**
- Supervised in UK by the Financial Conduct Authority, under the Payment Services Directive 2017 (FRN: **535954**).
- Registered with Data Protection
- Registered with HMRC MLR Number **XDML00000115193**

NOMINATED OFFICER (MONEY LAUNDERING REPORTING OFFICER) AND COMPLIANCE OFFICER

The Money Laundering Reporting Officer (also known as the nominated officer) contact information is:

Director / MLRO Name: **MR QAISAR SYED**
Phone: +44 020 8470 9333
Email: *alicoexchange@hotmail.com*

The MLRO is the focal point within the company for the oversight of all activity related to anti-financial crime issues. Their responsibilities include:

- carry out a risk assessment identifying where our business is vulnerable to money laundering and terrorist financing
- prepare, maintain and approve a written policy statement, controls and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- review and update the policies, controls and procedures to reflect changes to the risk faced by the business
- make sure there are enough trained people equipped to implement policies adequately, including systems in place to support them
- make sure that the policies, controls and procedures are communicated to and applied to branches in the UK
- monitor effectiveness of the business's policy, controls and procedures and make improvements where required
- we have systems to identify when we are transacting with high risk third countries identified by the EU or financial sanctions targets advised by HM Treasury and take additional measures to manage and lessen the risks

Acknowledgement:

This guidance is for directors, employees and Nominated Officers of Money Service Businesses who are the subject of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 and for whom HM Revenue & Customs (HMRC) is the supervisory authority

This guidance explains measures brought about by The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2019, which came into force on 10 January 2020. It is based on, and, where appropriate, replicates the guidance produced by the Joint Money Laundering Steering Group (JMLSG) for businesses that are supervised by the Financial Conduct Authority (FCA).

Purpose of this guidance:

The purpose of this guidance is to provide relevant businesses that are supervised by HMRC with comprehensive guidance on implementing the legal requirements for measures designed to deter, detect and disrupt money laundering and terrorist financing. It also provides guidance on complying with directions issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act 2008 and financial sanctions legislation.

CONTENTS OF THIS GUIDANCE

The guidance includes:

A definition of money laundering and terrorist financing

- The main pieces of UK legislation concerning AML/CTF
- The main legal obligations on relevant businesses under Money Laundering and Terrorist Financing (Amendment) Regulations 2019 the EC Wire Transfer/Payments Regulation and Counter-Terrorism Act
- The role of senior management in taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the business
- Information on the risk-based approach to the prevention of money laundering and terrorist financing
- The customer due diligence measures
- The evidence of identity requirements
- Methods for ongoing monitoring of business relationships
- Procedures for reporting suspicious activity
- Staff awareness and training requirements
- Record keeping requirements
- Details of criminal offences and penalties relating to money laundering, terrorist financing and the counter-terrorism act
- The sanctions for failure to comply with Money Laundering and Terrorist Financing (Amendment) Regulations 2019 and/or the counter-terrorism act
- Business sector specific material, which has been prepared principally by practitioners in the relevant sectors
- Information about directions issued by HM treasury under schedule 7 to the counter-terrorism act and what money service businesses will have to do once a direction has been issued.

Branches:

Alico UK Ltd currently has 4 branches and the senior management is committed to strictly monitor the compliance level of all branches with the policy and procedures of Alico UK Ltd. All branches have been frequently visited by internal and external compliance officers on regular basis to ensure that the branches are complying with company's policy and procedures on anti-money laundering, terrorist financing, fraud prevention, record keeping, and training.

Our branches are as follows:

1: Peckham

Unit 22, 137-139 Rye Lane Peckham London SE15 4ST Tel: 02072778598

2: East Ham

8 Station Parade, High Street North, East Ham E6 1JD

3: Southall

18B The Broadway, Southall UB1 IPS, T: 0205716661

4: Walthamstow

227 High Street , Walthamstow E17 7BH, T: 02085210999

COMPANY ANTI-MONEY LAUNDERING POLICY STATEMENT

It is the policy of ***ALICO UK LIMITED*** to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity.
We focus on developing a culture where the highest priority is given to ensure compliance with government regulations. This is helped by regular staff training to make sure they are aware of the law and their responsibilities.

We recognize that it is a legal requirement for us to notify the regulatory authorities whenever it has suspicions of any criminal activity by individuals engaged in a money transfer / foreign currency transaction.

The aim of the present policy is to communicate the importance for employees of reporting suspicious transactions and to underline the consequences of non-reporting.

The present policies are based on material made available by the relevant UK regulatory bodies. In particular a handbook produced by HM Customs and Revenue (HMRC) Money Service Businesses – Anti Money Laundering Guide and the Payment Services Regulations (2017) published by FCA.

This is the responsibility of all staff that are to report to the Money Laundering Reporting Officer**; MR QAISAR SYED** who will then report to the National Crime Agency (NCA)

…….

MR QAISAR SYED

DIRECTOR

WHAT IS MONEY LAUNDERING AND WHAT THE UK LAW REQUIRES

Within the broader financial crime agenda, we have identified money laundering, terrorist finance, sanctions list compliance, asset freeze issues and fraud prevention as the particular issues for our business, but we recognise that financial crime is an ever evolving challenge and that new kinds of financial crime threat are always arising, and will need to be addressed.

WHAT IS MONEY LAUNDERING?

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- **Placement:** Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

- **Layering:** Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

- **Integration:** Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering into arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) REGULATIONS 2019

The **2019 Money Laundering Regulations** include a number of new obligations on money service businesses. These include

- Obligation on those who run money transfer companies to satisfy a ‘fit and proper’ test - those not judged satisfactory will be prohibited from running money service businesses

- Customer ‘due diligence’ requirements – obligation to identify the customer and verify the customer from independent data source

- Special due diligence obligations for non-face to face customers and for customers who may be ‘politically exposed’

- Beneficial ownership – obligations to verify who are the underlying individuals who make financial gains from business relationships or transactions. Amendments to regulation 28 require firms to update their records relating to the beneficial ownership of corporate clients. Firms also need to understand the ownership and control structure of their corporate customers, and record any difficulties encountered in identifying beneficial ownership. Regulation 30A is a new requirement for firms to report to Companies House discrepancies between the information the firm holds on their customers compared with the information held in the Companies House Register.

- When a business relationship has been established, new requirements to establish customer source of funds/purpose of transaction

- Obligation to take a ‘risk based approach’ to all aspects of the AML policies for the business

The present policies are based on material made available by the relevant UK regulatory bodies. In particular Money Laundering and Terrorist Financing (Amendment) Regulations 2019 – transposing 5th AMLD, Anti Money Laundering Guide, Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation) and the Payment Services Regulations (2017).

New obligations on money service businesses according to 2019 Money Laundering Regulations include a number of. These include

- Obligation on those who run money transfer companies to satisfy a ‘fit and proper’ test - those not judged satisfactory will be prohibited from running money service businesses
- Customer ‘due diligence’ requirements – obligation to identify the customer and verify the customer from independent data source
- Special due diligence obligations for non-face to face customers and for customers who may be ‘politically exposed’
- **Beneficial ownership** – obligations to verify who are the underlying individuals who make financial gains from business relationships or transactions. Amendments to regulation 28 require firms to update their records relating to the beneficial ownership of corporate clients. Firms also need to understand the ownership and control structure of their corporate customers, and record any difficulties encountered in identifying beneficial ownership. Regulation 30A is a new requirement for firms to report to Companies House discrepancies between the information the firm holds on their customers compared with the information held in the Companies House Register.
- When a business relationship has been established, new requirements to establish customer source of funds/purpose of transaction
- Obligation to take a ‘risk-based approach’ to all aspects of the AML policies for the business

Policy of the company that all members of staff shall actively participate in preventing the services of the company from being exploited by criminals and terrorists for money laundering purposes. This

participation has as its objectives:

- Ensuring the company's compliance with all applicable laws, statutory instruments of regulation, and requirements of the company's supervisory body
- Protecting the company and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements
- Preserving the good name of the company against the risk of reputational damage presented
- By implication in money laundering and terrorist financing activities making a positive contribution to the fight against crime and terrorists

To achieve these objectives, it is the policy of this company that:

- Every member of staff shall meet their personal obligations as appropriate to their role and position in the company
- Commercial considerations shall never be permitted to take precedence over the company's anti-money laundering commitment

PAYMENT SERVICE REGULATION 2017

These Regulations may be cited as the Payment Services Regulations 2017.

The following provisions come into force on 13th August 2017—

(a) this regulation and regulations 2 (interpretation), 106 (functions of the FCA), 112(6) (policy on imposition of penalties), 118 (costs of supervision), 120 (guidance), 121

(FCA's exemption from liability in damages) and 147 (duty to co-operate and exchange of information);

(b) regulation 122 and the following provisions of Schedule 6 (application and modification of legislation)—

(i) paragraph 1 (disciplinary powers) in so far as that paragraph applies sections 69 and 70 of the 2000 Act;

(ii) paragraph 3 (FCA rules) for the purpose of enabling the FCA to make rules;

(iii) paragraph 5 (control over payment institutions) in so far as that paragraph applies the provisions of sections 179 and 191E of the 2000 Act which confer functions on the FCA;

(iv) paragraph 12 (application of the Financial Services and Markets Act 2000 (Service of Notices) Regulations 2001(h));

(c) regulation 156 in so far as it gives effect to the following provisions of Schedule 8 (amendments to legislation)—

(i) paragraph 2(6) (amendment of section 379A of the 2000 Act);

(ii) paragraph 3(b) (amendment of Schedule 15 to the Enterprise Act 2002(a));

(iii) paragraph 5 (amendment of the Electronic Money Regulations 2011(b)) for the purpose of enabling the FCA to impose requirements, give directions and make rules;

(d) for the purpose of enabling the FCA to impose requirements and give directions—

(i) regulation 5(3) and (5) (applications for authorisation as a payment institution);

(ii) regulation 6(7)(e) and (f) (professional indemnity insurance for authorised payment institutions);

(iii) regulation 11(1) and (3) (cancellation of registration);

(iv) regulation 13(1), (2), (3) and (5) (application for registration);

(v) regulation 15 (small payment institutions: supplementary provision) in so far as it applies regulation 11(1) and (3);

Schedule 5 (credit agreements).

(3) The following provisions come into force on 13th October 2017—

(a) Part 2, for the purposes of enabling—

(i) the making and determination of applications for authorisation or registration (including the imposition of requirements in relation to authorisations and registrations); and

(ii) the giving of notices under regulation 3(2) (exemption for municipal banks);

(b) for the purposes of enabling the giving of notifications and the making of applications to the FCA and enabling the FCA to take action in response to such notifications and applications, regulations 25 (outsourcing), 34 (use of agents) and 39 (notification of use of electronic communications exclusion);

In Schedule 6 (application and modification of legislation), paragraphs 2 (the Upper Tribunal), 5 (control over payment institutions) in so far as not already in force, 8 (restriction on disclosure of information), 10 (warning notices and decision notices) and 13 (application of the Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001);

(d) regulations 142 to 146 (misleading the FCA);

(e) regulation 150 (transitional and saving provisions), for the purposes of enabling the provision of information or giving of notification under regulation 150(3), and enabling the FCA to take action in response to such information or notification;

(f) regulation 156 in so far as it gives effect to—

(i) paragraph 5 of Schedule 8 (amendment of the Electronic Money Regulations 2011), for the purpose of enabling the giving of notifications, the making or determining of applications and the taking of action in response to such applications and notifications under the Electronic Money Regulations 2011;

(ii) paragraph 6 of Schedule 8 (amendment of the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975(a)), for the purpose of the FCA's determination of applications for authorisation or registration under Part 2 of these Regulations (including the imposition of requirements in relation to authorisations and registrations).

(4) Regulations 27 (notice of intention) and 28 (decision following notice of intention) come into force on 13th December 2017 for the purposes of enabling the giving of notifications and enabling the FCA to take action in response to such notifications.

(5) Regulations 68(3)(c), 69(2)(a) and (3)(d), 70(2)(a) and (3)(c), 77(4)(c) and (6) and 100 (secure communication and authentication) come into force eighteen months after the date on which the regulatory technical standards adopted under Article 98 of the payment services directive come into force.

(6) Except as provided in paragraphs (2) to (5), these Regulations come into force on 13th January 2018.
(7) Paragraph 6 of Schedule 8 (amendment of the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975) extends to England and Wales only.

CRIMINAL FINANCES ACT 2017

An Act to amend the Proceeds of Crime Act 2002; make provision in connection with terrorist property; create corporate offences for cases where a person associated with a body corporate or partnership facilitates the commission by another person of a tax evasion offence; and for connected purposes.

Power to extend moratorium period

(1) Part 7 of the Proceeds of Crime Act 2002 (money laundering) is amended as follows.

(2) In section 335 (appropriate consent), after subsection (6) insert— "(6A)

Subsection (6) is subject to—

(a) section 336A, which enables the moratorium period to be extended by court order in accordance with that section, and

(b) section 336C, which provides for an automatic extension of the moratorium period in certain cases (period extended if it would otherwise end before determination of application or appeal proceedings etc)."

(3) In section 336 (nominated officer: consent), after subsection (8) insert— "(8A)

Subsection (8) is subject to—

(a) section 336A, which enables the moratorium period to be extended by court order in accordance with that section, and section 336C, which provides for an automatic extension of the moratorium period in certain cases (period extended if it would otherwise end before determination of application or appeal proceedings etc)."

(4) After section 336 insert—

Power of court to extend the moratorium period - 336A

(1) The court may, on an application under this section, grant an extension of a moratorium period if satisfied that—

(a) an investigation is being carried out in relation to a relevant disclosure (but has not been completed),

(b) the investigation is being conducted diligently and expeditiously,

(c) further time is needed for conducting the investigation, and

(d) it is reasonable in all the circumstances for the moratorium period to be extended.

(2) An application under this section may be made only by a senior officer.

(3) The application must be made before the moratorium period would otherwise end.

(4) An extension of a moratorium period must end no later than 31 days beginning with the day after the day on which the period would otherwise end.

(5) Where a moratorium period is extended by the court under this section, it may be further extended by the court (on one or more occasions) on the making of another application.

(6) A moratorium period extended in accordance with subsection (2) or (4) of section 336C may also be further extended by the court on the making of an application under this section.

(7) But the court may not grant a further extension of a moratorium period if the effect would be to extend the period by more than 186 days (in total) beginning with the day after the end of the 31 day period mentioned in section 335(6) or (as the case may be) section 336(8).

(8) Subsections (1) to (4) apply to any further extension of a moratorium period as they apply to the first extension of the period under this section.

(9) An application under this section may be made by an immigration officer only if the officer has reasonable grounds for suspecting that conduct constituting the prohibited act in relation to which the moratorium period in question applies—

(a) relates to the entitlement of one or more persons who are not nationals of the United Kingdom to enter, transit across, or be in, the United Kingdom (including conduct which relates to conditions or other controls on any such entitlement), or

(b) is undertaken for the purposes of, or otherwise in relation to, a relevant nationality enactment.

(10) In subsection (9)—

"prohibited act" has the meaning given by section 335(8) or (as the case may be) section 336(10);

WHAT ARE THE OFFENCES AND PENALTIES?

THE PROCEEDS OF CRIME ACT 2002 (POCA) AS AMENDED BY THE SERIOUS ORGANISED CRIME AND POLICE ACT 2005

POCA Part 7 sets out the primary offences relating to money laundering. There are three principal money laundering offences covering criminal activity and four related money-laundering offences.

These are shown in the table below:

No	An offence is committed under POCA when a person
1	conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the proceeds of crime which the person knows or suspects represents the proceeds of crime (POCA section 327) But an offence has not been committed under this section if - * he makes an authorised disclosure under section 338 and has the appropriate consent or he intended to make such a disclosure but had a reasonable excuse for not doing so or the act he has done is done in carrying out a function he has done relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefitting from criminal conduct.
2	enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (POCA section 328) But an offence has not been committed under this section if - (*same as above)
3	acquires, uses or has possession of property which he knows or suspects represents the proceeds of crime (POCA section 329) But an offence has not been committed under this section if - (*same as above) ** with the addition of that he acquired or used or had possession of the property for adequate consideration;
4	fails to disclose to the MLRO (in the regulated sector), knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering – this applies to any individual at whatever level (employee, manager, director) (POCA section 330) But an offence has not been committed under this section if – he has a reasonable excuse for not disclosing the information or other matter or he is a

	professional legal adviser and the information or other matter came to him in privileged circumstances or that he does not know or suspect that another person is engaged in money laundering or he has not been provided by his employer with such training as is specified by the Secretary of State by order for the purposes of this section.or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to any individual at whatever lever (employee, manager, director) (POCA section 330)
5	fails to disclose to NCA (in the regulated sector), knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to the MLRO or sole proprietor of a business (POCA section 330) But an offence has not been committed under this section if he has a reasonable excuse for not disclosing the information or other matter.
6	A person commits an offence if – he knows or suspects that another person is engaged in money laundering or that the information or other matter on which his knowledge or suspicion is based came to him in consequence of a disclosure made under section 337 or 338 of the Act, or that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him. But an offence has not been committed under this section if he has a reasonable excuse for not disclosing the information or other matter
7	A person commits an offence if – He knows or suspects that a disclosure falling within section 337 or 338 of the Act has been made, and he makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure. But an offence has not been committed under this section if –

Penalties:

A person found guilty of an offence under sections 327, 328 or 329 is liable to on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.

A person found guilty of an offence under sections 330, 331, 332 or 333 is liable to on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Regulator: National Crime Agency

WHAT IS TERRORISM

Terrorism is the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

The definition of 'terrorist property' means that all dealings with funds or property which are likely to be used for the purposes of terrorism, even if the funds are 'clean' in origin, is a terrorist financing offence.

For the purposes of this guidance, references to terrorist financing includes proliferation financing which is assisting in the financing and/or development of nuclear, biological, radiological, chemical weapons and/or their means of delivery.

Money laundering and terrorist finance offences are committed, however small the amount involved.

The UK legislation on money laundering applies to the proceeds of conduct that is an offence in the UK, and most conduct occurring elsewhere that would have been an offence if it had taken place in the UK.

WHAT IS A DIRECTION ISSUED UNDER SCHEDULE 7 TO THE COUNTER-TERRORISM ACT 2008 (A 'DIRECTION')?

The Terrorism Acts (2000) as amended by the Anti-Terrorism, Crime and Security Act 2001:

These acts set out the primary offences relating to the funding of terrorism. The Acts deal with suspicion of terrorist financing and requires firms in the regulated sectors to report where there are grounds to know or suspect offences relating to terrorist financing. These offences include:

- fundraising for the purpose of terrorism (section 15)
- using or possessing money for the purposes of terrorism (section 16)
- involvement in funding arrangements (section 17); and
- money laundering (facilitating the retention or control of money which is destined for, or is the proceeds of, terrorism) (section 18)

This obligation is significantly different from that under POCA – as it does not just cover "proceeds" of crime, but all funds, regardless of their origin.

Penalties: Conviction for any of the above offences can incur up to 14 years imprisonment and/or an unlimited fine. Failure to disclose the belief or suspicion that someone has committed any of the offences above can incur up to five years imprisonment and/fines. It is likewise an offence to 'tip off' a suspect that a disclosure has been made of suspicion of terrorist funding or of a subsequent investigation. This offence carries a penalty of up to two years in prison and/or unlimited fines.

Regulator: Responsibility for dealing with criminal breaches of the Terrorism Act lies with the police but businesses which follow guidance issued by HMRC are likely to have protection in a court of law.

COUNTER TERRORISM ACT 2008 SCHEDULE 7

This schedule provides new powers for the Treasury to apply financial restrictions in respect of non-EEA countries because of the risk posed by money laundering or terrorist financing, either:

- in accordance with a recommendation of the Financial Action Task Force (see www.fatf-gafi.org)
- or on its own initiative

- if such activity poses a significant risk to the UK's national interests

The provisions of the act allow HM Treasury to impose on firms:

- stricter requirements for Customer Due Diligence – identifying clients, beneficial owners and the nature of business relationships
- stricter requirements for on-going monitoring of transactions a requirement to undertake systematic reporting of all transactions with designated entities
- a requirement to limit or stop business with designated entities

Companies which wish to be notified about Orders issued under the CTA 2008 should sign up at the following address- http://www.hm-treasury.gov.uk/fin_crime_mailinglist.htm

Penalties: There are civil and criminal sanctions for failure to comply with the Counter Terrorism Act 2008 Schedule 7. These include unlimited fines and imprisonment for up to two years.

Regulator: HM Revenue and Customs

WHAT IS THE FINANCIAL ACTION TASK FORCE (FATF)?

FATF is an inter-governmental body which develops international standards to combat money laundering and terrorist financing. It also produces lists of countries that do not have sufficient legal and regulatory standards to combat money laundering and terrorist financing.

WHAT ARE SANCTIONS?

Financial Sanctions

These are normally used by the international community for one or more of the following reasons:

- To encourage a change in the behaviour of a target country or regime
- To apply pressure on a target country or regime to comply with set objectives
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed
- To prevent and suppress the financing of terrorists and terrorist acts

In the UK, HM Treasury is responsible for publishing the list of individuals/groups to which financial sanctions apply and for monitoring compliance.
The HM Treasury consolidated Sanctions List is available from: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

Penalties: It is a criminal offence to make funds available to individuals/groups on the HMT Financial Sanctions list. This includes dealing directly with them or through intermediaries (such as lawyers or accountants). The maximum term of imprisonment for criminal contravention of the Financial Sanctions regime is currently seven years.

Regulator: Asset Freezing Unit, HM Treasury

BRIBERY OFFENCES AS PER BRIBERY ACT 2010 AND PENALTIES:

1. Offences of bribing another person:

(1) A person ("P") is guilty of an offence if either of the following cases applies.
(2) Case 1 is where—
(a) P offers, promises or gives a financial or other advantage to another person, and
(b) P intends the advantage—
(i) To induce a person to perform improperly a relevant function or activity, or
(ii) To reward a person for the improper performance of such a function or activity.
(3) Case 2 is where—
(a) P offers, promises or gives a financial or other advantage to another person, and
(b) P knows or believes that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity.
(4) In case 1 it does not matter whether the person to whom the advantage is offered, promised or given is the same person as the person who is to perform, or has performed, the function or activity concerned.
(5) In cases 1 and 2 it does not matter whether the advantage is offered, promised or given by P directly or through a third party.

2. Offences relating to being bribed
3. Function or activity to which bribe relates
4. Improper performance to which bribe relates
5. Expectation test
6. Bribery of foreign public officials
7. Failure of commercial organisations to prevent bribery:

(1) A relevant commercial organisation ("C") is guilty of an offence under this section if a person ("A") associated with C bribes another person intending—
(a) To obtain or retain business for C, or
(b) To obtain or retain an advantage in the conduct of business for C.
(2) But it is a defence for C to prove that C had in place adequate procedures designed to prevent persons associated with C from undertaking such conduct.
(3) For the purposes of this section, A bribes another person if, and only if, A—
(a) Is, or would be, guilty of an offence under section 1 or 6 (whether or not A has been prosecuted for such an offence), or
(b) Would be guilty of such an offence if section 12(2)(c) and (4) were omitted.
(4) See section 8 for the meaning of a person associated with C and see section 9 for a duty on the Secretary of State to publish guidance.
(5) In this section—
"Partnership" means—
(a) A partnership within the Partnership Act 1890, or
(b) A limited partnership registered under the Limited Partnerships Act 1907, or a firm or entity of a similar character formed under the law of a country or territory outside the United Kingdom,

"Relevant commercial organization" means—
(a) A body which is incorporated under the law of any part of the United Kingdom and which carries on a business (whether there or elsewhere),
(b) Any other body corporate (wherever incorporated) which carries on a business, or part of a business, in any part of the United Kingdom,

(c) A partnership which is formed under the law of any part of the United Kingdom and which carries on a business (whether there or elsewhere), or
(d) Any other partnership (wherever formed) which carries on a business, or part of a business, in any part of the United Kingdom, and, for the purposes of this section, a trade or profession is a business.

PENALTIES

(1) An individual guilty of an offence under section 1, 2 or 6 is liable—
(a) on summary conviction, to imprisonment for a term not **exceeding 12 months, or to a fine not exceeding the statutory maximum, or to both,**
(b) On conviction on indictment, to imprisonment for a term **not exceeding 10 years, or to a fine, or to both.**
(2) Any other person guilty of an offence under section 1, 2 or 6 is liable—
(a) On summary conviction, to a fine not exceeding the statutory maximum,
(b) On conviction on indictment, to a fine.

(3) A person guilty of an offence under section 7 is liable on conviction on **Indictment to a fine.**

[For details: http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf**]**

Fraud Policy

What is Fraud?

No precise legal definition of fraud exists; many of the offences referred to as fraud are covered by the Theft Acts in England and Wales, and under Common Law in Scotland. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. Other offences are created by more sector-specific laws such as those that prohibit corruption or create offences related to companies or financial services, for example.

For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation, or causing loss to another party. This most often occurs in the context of a relationship with a customer, client, or colleague on an individual or organisational basis.

There are four basic ingredients which are necessary for a fraud to occur:

- People to carry out the fraud
- Assets to acquire
- Intent to commit the fraud
- Opportunity

While some people would never contemplate perpetrating a fraud, others might do so if they think they can get away with it. Fraudsters are usually alert, plausible and calculating. Company can deter a fraudster who might want to take advantage of company personally, or our business, by being alert to the possibilities. Alertness and effective controls will increase the chances of being caught and will thus act as a deterrent.

In business some frauds arise because of a system weakness, such as a lack of proper control over placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be carelessness in carrying out a check. It may be that too much trust has been placed in one individual with no effective separation of duties. Frauds which result from collusion may be more difficult to prevent. A computer can be instrumental in the perpetration of the fraud because of the absence of human review of transactions. The lack of human involvement may allow transactions to be processed which would have been queried in a manual system. An organisation can therefore be exposed to the risk of fraud in a number of different ways. For the purpose of this guide we can divide fraud into three categories:

Internal fraud:

This is fraud perpetrated by individuals inside the organisation and is most often carried out by staff who have access to liquid or moveable assets. It is likely that the risk of fraud and its scale will increase if the member of staff is able to conceal the irregularities by also having access to accounting records. It may be opportunistic, though it may also be planned and committed over a long period.

External fraud:

This is fraud which is perpetrated by individuals outside the organisation and covers activities such as theft, deception and computer hacking. It is very often committed as a result of inadequate safeguards.

Collusion:

This type of fraud involves two or more parties, either both internal, or internal and external, working together. This type of fraud can be difficult to detect as controls may at first appear to be working satisfactorily.

The pages that follow illustrate real cases and identify topical scams. Advice, based on this experience suggests ways of preventing fraud happening to you.

Types of Fraud

Frauds can be categorised by the type of victim involved. The most common groups of victims encountered by investigators include:

- Investors
- Creditors
- Businesses
- Banks or other financial institutions
- Central or local government
- Fraud by manipulating financial markets

Frauds can also be categorised by the technique or activity used by the fraudster. These include:

- Advance fee frauds
- Bogus invoices

- Computer hacking of information or property
- Corruption and bribery
- Counterfeiting, forgery, or copyright abuse
- Credit Card fraud
- False Accounting - manipulation of accounts and accounting records
- Fraudulent bankruptcy - exploitation of cross-border corporate structures
- Insurance fraud
- Internet online scams - auctions, credit card purchases, investment scams
- Investment fraud
- Long Firm fraud
- Misappropriation of assets
- Money laundering
- Mortgage Fraud
- Payroll fraud
- Principal agents - failure of systems to restrict key individuals
- Pyramid schemes
- Unsolicited letter frauds

For update information on issues related to fraud, reference should be made to the Fraud Reduction website published by the National Working Group on Fraud on behalf of the UK Association of Chief Police Officers (ACPO). This is available at: www.fraud-stoppers.info.

Regulatory Guidance

Firms which follow 'relevant guidance' issued by the appropriate regulator will have a defence against any accusation of non-compliance with the law. For the purposes of money transfer businesses, companies which comply with guidance issue by HM Revenue and Customs will have protection in relation to 2017 Money Laundering Regulations, EU Payments Regulation, Terrorism Act 2000, Counter Terrorism Act 2007, Section 7 and the Proceeds of Crime Act 2002.

HMRC has issued guidance (MLR8) which was formalised with effect from 12/09/2008. MLR8 is available on the HMRC website: http://www.hmrc.gov.uk/mlr/latest-news.html

Companies should also review guidance issued by the Joint Money Laundering Steering Group to firms regulated by the FCA for AML. This is available at: www.jmlsg.org.uk.

What does UK Financial Crime legislation mean for us?

The combined objective of all legislation and regulation is to make it difficult for criminals and terrorists to operate through the international financial system.

The combined impact of these laws for our company is to make it an offence for any employee, branch employee to provide assistance to another person to obtain, conceal, retain or invest proceeds of crime if the employee, agent or agent employee knows or suspects or, in some cases, (i.e. terrorist funding or the offences of concealing or transferring), should have known or suspected, that the other person has been engaged in, or has benefited from, criminal conduct or, alternatively, is involved in assisting terrorist activity.

KYC PROCESS AND CUSTOMER ONBOARDING / CUSTOMER DUE DILIGENCE (CDD)

This section sets out and explains the legal definitions and detailed requirements for customer due diligence under the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 and the Counter-Terrorism Act 2008. Regulation applies when a relevant person is required by regulation 27 to apply customer due diligence measures explains the principles and criteria to be applied to obtaining and verifying evidence of customers' identity.

What is customer due diligence?

The meaning and application of customer due diligence is set out in Money Laundering and Terrorist Financing (Amendment) Regulations 2019 regulation 27 and paragraph 10 of Schedule 7 to the Counter-Terrorism Act 2008.

These regulations require businesses to:
This regulation applies when a relevant person is required by regulation 27 to apply customer due diligence measures.

- The relevant person must—identify the customer unless the identity of that customer is known to, and has been verified by, the relevant person;
- verify the customer's identity unless the customer's identity has already been verified by the relevant person; and
- assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

CUSTOMER DUE DILIGENCE – PRIVATE CLIENT

PROCEDURE OF ALICO UK LIMITED REGARDING CDD:

Customer approach to ALICO UK LIMITED Office/Branch for the purpose to do remittance transaction, It is responsibility of ALICO UK LIMITED representative to Identify customer through ID which is acceptable according to ALICO UK LIMITED policy, after obtaining ID and Documents Customer Service officer (CSO)/branch initiate transaction and post it to system.

All the Transaction is done by centralised IT Software, each and every transaction is gone for approval to Head Office, all the transactions shows in Head office system as pending, Head office (MLRO) check transactions and approved transaction. After approval it is ready to collect from correspondent office by beneficiary by showing photo ID.

If there is some issue with transaction then Head office hold the transaction unless it is resolved.

Please note, the easiest way to get certified customer ID is to use the 'Identity Checking service' at the UK post office . For more details see: http://www.postoffice.co.uk/document-certification-service

Identifying individuals

As part of customer due diligence measures, identify individuals, should obtain a private individual's full name, date of birth and residential address as a minimum.

We verify these using current government issued documents with the customer's full name and photo, with a customer's date of birth or residential address such as:

- a valid passport
- a valid photo card driving licence (full or provisional)
- a national identity card

When verifying the identity of a customer using the above list of government-issued documents, should take a copy and keep it in the customer's file.

Where the customer doesn't have one of the above documents may wish to ask for the following:

- a government issued document (without a photo) which includes the customer's full name and also secondary evidence of the customer's address, for example driving licence or recent evidence of entitlement to state or local authority funded benefit such as housing benefit, council tax benefit, pension, tax credit
- secondary evidence of the customer's address, not downloaded from the internet, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement

Verification of the customer's identity by documents, must see the originals and not accept photocopies, nor accept downloads of bills as described below:

- photocopied identity documents can be accepted as evidence provided that each copy document has an original certification by an appropriate person to confirm that it is a true copy and the person is who they say they are

- for standard customer due diligence an appropriate person is, for example, a bank, financial institution, solicitor or notary, independent professional person, a family doctor, chartered accountant, civil servant, or minister of religion

The documents must be from a reliable source not connected to the customer.

Should be check the documents to satisfy yourself of the customer's identity. This may include checking:

- spellings
- validity
- photo likeness
- whether addresses match

Customer Due Diligence

Why is it necessary to apply CDD measures?

Our CDD obligations are designed to make it more difficult for our business to be used by criminals for money laundering or terrorist financing. We must also guard against fraud, including impersonation fraud. Where there is a business relationship, CDD measures must involve more than just determining the customer's identity. We must also ascertain the intended nature and purpose of the business relationship and collect information on the customer, his business and risk profile to allow ongoing monitoring of the business relationship to ensure that transactions undertaken are consistent with that knowledge.

What is customer due diligence?

For ALICO UK LIMITED, CDD means identifying our customers and verifying their identity.

When must these due diligence measures be applied?

CDD measures must be applied:

- when establishing a business relationship;
- where there is a suspicion of money laundering or terrorist financing;
- where there are doubts about previously obtained customer identification information;
- at appropriate times to existing customers on a risk-sensitive basis.

Determining the extent of customer due diligence measures

The Money Laundering Regulations require that the extent of CDD measures must be decided on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. Company must be able to demonstrate to the OFT that our due diligence measures are appropriate in view of the risk of money laundering and terrorist financing that we face.

Noncompliance with CDD measures

If we are unable to comply with the required CDD measures, we must not carry out the requested transaction, not establish a business relationship, terminate any existing business relationship with the customer, and consider making a report to NCA.

Enhanced Due Diligence, EDD

What is Enhanced Due Diligence?

Enhanced due diligence applies in situations that are high risk. It means taking additional measures to identify and verify the customer identity and source of funds and doing additional ongoing monitoring.

Company does this when:

- We have identified in our risk assessment that there is a high risk of money laundering or terrorist financing
- HMRC or another supervisory or law enforcement authority provide information that a particular situation is high risk
- a customer or other party is from a high risk third country identified by the EU
- a person has given false or stolen documents to identify themselves (immediately consider reporting this as suspicious activity)
- a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex, unusually large or with an unusual pattern and have no apparent legal or economic purpose

Customers:

Customer factors based on information have or behaviours indicating higher risk, such as:

- unusual aspects of a business relationship
- a person is resident in a high risk area
- use of a legal person or arrangement used to hold personal assets
- a company with nominee shareholders or share in bearer form
- an unusual or complex company structure given the nature of the type of business
- searches on a person or associates show, for example, adverse media attention, disqualification as a director or convictions for dishonesty

How the transaction is paid for or specific requests to do things in a certain way may indicate higher risk, for example:

- Use of private banking
- anonymity is preferred
- a person is not physically present
- payment from third parties with no obvious association
- involves nominee directors, nominee shareholders or shadow directors, or a company formation is in a third country

Geographical factors indicating higher risk, including:

- Countries identified by a credible source as:
    - not subject to equivalent anti-money laundering or counter terrorist measures

- with a significant level of corruption, terrorism or supply of illicit drugs
- subject to sanctions or embargoes issued by EU or UN
- providing funding or support for terrorism
- having organisations designated as "proscribed" by the UK
- having terrorist organisations designated by the EU, other countries and international organisations

Beneficiaries:

- If the purpose of sending is family support, Analyze location of collection of Beneficiary's to understand the cost of livings of beneficiaries and/or related family member.
- If the purpose of something other reason, analyze the purpose is reasonable as per available data and information of the sender and beneficiaries.

ONGOING MONITORING OF TRANSACTIONS

We continue to monitor a business relationship after it is established. We monitor transactions, and where necessary the source of funds, to ensure they are consistent with what we have in our Threshold. We also keep the information we collect for this purpose is up-to-date. It is checked on regular basis and expired documents replaced with copies of newly issued documents.

Occasional transaction

An occasional transaction is a transaction of (or the sterling equivalent) that is not part of an ongoing business relationship. It also applies to a series of transactions totalling £10,000 or more, where there appears to be a link between transactions (linked transactions).

Ongoing monitoring of Customers

We also manually review the customer's pattern of behavior, looking for any signs of suspicious activity such as:

- Is the pattern of transactions consistent and regular?
- Are the size and frequency of recent transactions consistent with the normal activities of the customer.
- Has the pattern of transactions changed since the person first became a customer?
- Are there sudden increases in the frequency or value of a customer's transactions without reasonable explanation?
- Is there a significant and unexpected improvement in the customer's financial position, which the customer is unable to explain satisfactorily?
- Does a third party make repayments on behalf of the customer without a satisfactory explanation?

- Are there frequent address changes?

Ongoing Monitoring of ID Documents

Documentary evidence of an individual's identity issued by a government department or agency, when verifying identity using documents (as opposed to electronic checks), the documents should be:
Either a government-issued document which incorporates the customer's full name and photograph, and either his or her residential address or date of birth, such as:

Valid passport
Valid driving license (full or provisional)
National ID card (for EU nationals)
Firearms certificate or shotgun licence

This must be supported by secondary evidence of ID, which incorporates the customer's full name and residential address and Date, such as:

Current council tax letter or statement
Current bank or credit/debit card statements
Utility bills

These other documents are intended to confirm a customer's address, so they should have been delivered to the customer through the post, rather than being accessed by him from the internet. Whichever documents are used, we must check them carefully. For example, checks on photo ID may include:

- Does the date of birth on the evidence match the apparent age of the customer in the photo?
- Is the ID valid?
- Is the spelling of names the same as other documents provided by the customer?

Checks on secondary evidence of ID may include:

- Do the addresses match the address given on the photo ID?
- Does the name of the customer match the name on the photo ID?

We also consider whether the documents may be forged. In all cases where customers are unable to provide the standard evidence, we must establish and document the reasons for this. Some categories of

financially-excluded customers may represent a higher risk of money laundering, so we consider enhanced monitoring of these customers' transactions.

Extent of Customer due Diligence Measures

The extent of customer due diligence measures depends on the degree of risk. It depends on the type of customer, business relationship, product or transaction.

It goes beyond simply carrying out identity checks, this is because even people we already know well may become involved in illegal activity at some time, for example if their personal circumstances change or they face some new financial pressure. our due diligence measures should reduce the risk of this, and the opportunities for staff to be corrupted.

- We consider the level of identification, verification and ongoing monitoring that's necessary, depending on the risk you assessed.

OBTAINING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF A BUSINESS RELATIONSHIP:

What is a business relationship?

A business relationship exists where the company sets up a process with the customer which makes it easier for them to make regular transactions. It is our company policy that a business relationship exists in one of the following situations:

- a unique customer number is allocated and a customer registration form is completed
- customers are able to deposit into the company bank account
- customers can make transactions by telephone or over the internet

In situations where a business relationship exists, there is an obligation to obtain a proof of ID, plus confirmation of purpose of transaction and source of funds. There is an obligation on the company to monitor all transactions carried out in the business relationship.

What information is required?

Depending on the business's risk assessment of the situation, information that might be relevant to obtain to understand the purpose and intended nature of the relationship may include some or all of the following:

- details of the customer's business or employment
- the expected source and origin of the funds to be used in the relationship
- copies of recent and current financial statements
- the nature and purpose of relationships between signatories and underlying beneficial owners
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

OCCASIONAL TRANSACTIONS

General legal requirements:

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 requires that customer due diligence measures must be applied when a business carries out occasional transactions. As defined in The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, occasional transaction means a transaction (carried out other than as part of an ongoing business relationship) amounting to 15,000 euro or more, (or the equivalent in any currency) whether the transaction is carried out in a single operation or several operations which appear to be linked.

Linked Transactions

It is company policy that transactions are 'linked' when the following criteria apply:

i. The same sending customer has sent 15,000 Euros (or local equivalent) or more in the last three months to the same receiving customer in a number of individual transactions
ii. Three sending customers or more are sending to the same receiving customer (or receiving address or receiving telephone number) AND the receiving customer or bank account has received more than 15,000 Euros (or local equivalent) in last 3 three months
iii. A sending customer is sending funds on behalf of one or several people (see under CDD – private client)
iv. In the event that 'linked' transactions are identified, they should be notified to the MLRO who will determine whether or not there are any suspicious circumstances which mean the transaction should be reported to NCA.

ENHANCED DUE DILIGENCE (EDD) POLICY

Money Laundering and Terrorist Financing (Amendment) Regulations 2019 requires businesses to apply enhanced due diligence measures on a risk-sensitive basis:

A relevant person of ALICO UK LIMITED must apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the customer due diligence measures required under regulation 28 and, if applicable, regulation 29, to manage and mitigate the risks arising—

(a) in any case identified as one where there is a high risk of money laundering or terrorist financing—
  (i) by the relevant person under regulation 18(1), or
  (ii) in information made available to the relevant person under regulations 17(9) and 47;
(b) in any business relationship or transaction with a person established in a high-risk third country;
(c) in relation to correspondent relationships with a credit institution or a financial institution (in accordance with regulation 34);
(d) if a relevant person has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP (in accordance with regulation 35);
(e) in any case where the relevant person discovers that a customer has provided false or stolen identification documentation or information and the relevant person proposes to continue to

deal with that customer;

(f) in any case where—

(i) a transaction is complex and unusually large, or there is an unusual pattern of transactions, and

(ii) the transaction or transactions have no apparent economic or legal purpose, and

in any other case which by its nature can present a higher risk of money laundering or terrorist financing.

POLITICALLY EXPOSED PERSONS (PEPS) CHECK

The definition of 'PEP' is set out below:

Politically exposed persons are persons that are entrusted with prominent public functions, held in the UK or abroad. Typically this includes:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or similar bodies
- members of the governing bodies of political parties
- members of supreme and constitutional courts and other high level judicial bodies
- members of courts of auditors or boards of central banks
- ambassadors, and high ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state owned enterprises
- directors , deputy directors and members of the board, or equivalent of an international organisation

The definition includes family members such as spouse, partners, children (of the person and their spouse or partner) and parents and known close associates. Close associates are persons who have:

- joint legal ownership, with a politically exposed person, of a legal entity or arrangement
- any other close business relationship with a politically exposed person
- sole beneficial ownership of a legal entity or arrangement set up for the benefit of a politically exposed person

How can PEP be identified?

Under the Money Laundering Regulations, businesses must have risk-sensitive policies and procedures in place that can identify when a customer with whom they propose to have a business relationship or carry out an occasional transaction (that is, of 15,000 euro or more) is a politically exposed person. Where there is a risk that such a customer may be a politically exposed person, businesses should make appropriate enquiries by, for example, asking the customer for background information, researching publicly available information via the Internet, or, if the risk is substantial, consulting a commercial website listing politically exposed persons. If there is doubt about whether the customer is a politically exposed person, the customer should be treated as high risk.

In deciding whether a person is a known close associate of a politically exposed person businesses need only have regard to information that they hold or is publicly known.

It is a matter of company policy that all customers will be required to indicate whether they or any member of their family has previously worked in a non EU country at any time in the preceding 12

months. In case the answer is yes, the cashier must make enquiries to establish whether the customer may meet the criteria for being 'politically exposed'.

In cases where PEP is identified:

If the customer is a politically exposed person, family member or known close associate of one, then we put in place the following enhanced due diligence measures:

- obtain senior management approval before establishing a business relationship with that person
- take adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship or transaction
- conduct enhanced ongoing monitoring where We've entered into a business relationship

We continue to apply enhanced due diligence when the politically exposed person has left the function or position and for a further period of 12 months.

For family members and close associates the obligation to apply enhanced due diligence stops as soon as the politically exposed person no longer holds the office.

- We assess the level of risk that the politically exposed person presents and apply an appropriate level of enhanced due diligence.

SANCTIONS LIST CHECK

The company has developed a policy to check all transactions to confirm that no transaction involves any individual or company on the UK Sanctions list. (HM Treasury Consolidated List).

This list is available at: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

In the situation that there is any target match, the transaction would be automatically frozen and a report will be made to HM Treasury (Asset Freezing Unit) by the MLRO. The details of the Asset Freezing Unit are as follows:

Asset Freezing Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ
E-mail: assetfreezingunit@hm-treasury.gov.uk
Fax: 020 7270 5430
Telephone: 020 7270 5664 or 020 7270 5454

The transaction will also be reported to National Crime Agency (NCA)

If and when the company processes USD$ to settle payments, it is company policy that all beneficiaries of transactions processed in USD$ are verified against the Office of Foreign Asset Control (OFAC) list. In any case where a target match is found, the transaction will not be allowed to proceed.

REPORTING SUSPICIOUS ACTIVITY

What is suspicious activity (which must be reported)?

This is the name given to a report sent to the NCA under the Proceeds of Crime Act or the Terrorism Act. The report identifies individuals, or an employee, suspect may be involved in laundering money or financing terrorism. The term suspicion is meant to be applied in its everyday, normal sense. But if still not sure of the meaning of suspicious, then the courts have said that 'it is a possibility that is more than fanciful'.

The suspicion is that the funds or property involved in the transaction is the proceeds of any crime or linked to terrorist activity. Do not have to know what sort of crime may have been committed, but one or more warning signs of money laundering, which cannot be explained by the customer, will be relevant.

Suspicious activity reports – internal company process

As part of internal suspicious reporting, Alico UK Limited's Staff or Branch staff make internal reports and report to MLRO for review. After review if MLRO still thinks suspicion of staff is valid then MLRO reports to NCA.

As a money service business in the regulated sector, Alico UK Limited also required to make a Suspicious Activity Report (SAR) as soon as possible after Company know or suspect that money laundering or terrorist financing is happening. This means that the facts Company has about the persons involved and the transaction would cause a reasonable person in our position to have a suspicion.

Company submits a suspicious activity report to the NCA by NCA online portal.

We submit a suspicious activity report to the NCA by registering with the NCA online. The NCA provide information and registration details online and the NCA prefers this method. The system doesn't retain a file copy for use, so we may wish to keep a copy of our report but this must be securely kept. This system lets:

- register your business and contact persons
- receive a welcome pack with advice and contact details
- submit a report at any time of day
- receive email confirmation of each report.

Submitting a request for a defence to the NCA, whether we are granted a defence, or not, does not replace the requirement on the business to complete customer due diligence before entering into a business relationship (see Defence SAR below). It is important that we have detailed policies, controls and procedures on internal reporting and the roll of the nominated officer.

Company provide regular training for staff in what suspicious activity may look like in our business and keep records of that training, who has received it and when. The nominated officer must be conversant with guidance on how to submit a report and in particular be aware of the codes detailed in the glossary that must be used in each report.

A suspicious activity report must be made to the NCA no matter what part of business the suspicion arises in. The tests for making a report about terrorist financing are similar. We make a report if suspect or had

reasonable grounds for knowing or suspecting that another person committed or attempted to commit a terrorist financing offence.

In the situation that an employee, agent or agent employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company MLRO is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Activity Report Form'.

The SAR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc.)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the MLRO to discuss the reasons for their suspicion – however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below).

The timing for submitting the internal SAR is important. The law states that an individual working in the regulated sector (i.e. a money transfer company) should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the Financial Intelligence Unit at the National Crime Agency (NCA) to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company MLRO.

Once the MLRO receives the internal SAR from the staff member, the MLRO has two options:

- Report the SAR on to National Crime Agency (see procedure below)
- File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to NCA.

The MLRO should complete the MLRO SAR Resolution form (see appendix for sample) in the event he decides not to make a report to NCA.

MAKING A SUSPICIOUS ACTIVITY REPORT TO NCA

A suspicious activity report (SAR) is the name given to the making of a disclosure to NCA under either Proceeds of Crime Act or the Terrorism Act. NCA has issued a preferred form to be completed when

making a SAR, which may become mandatory in the future. NCA encourages firm to start using the preferred form now.

Preferably, Company use SARs Online (https://www.ukciu.gov.uk/saronline.aspx) where have computer access. This securely encrypted system provided by NCA allows firms to:

- register the firm and relevant contact persons
- submit a SAR at any time of day
- receive e-mail confirmations of each SAR submitted

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. Firms will not receive acknowledgement of any SARs sent this way.

Firms can contact NCA on this number for:

- help in submitting a SAR or with the SARs online system
- help on consent issues
- assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation

NCA is required to treat any SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their firm is not disclosed to other persons.
It is our company policy that only the MLRO can submit a SAR to NCA.

It is expressly forbidden for employees to make a SAR direct to NCA.

Dealing with the National Crime Agency

The disclosure regime for money laundering and terrorist financing is run by the financial intelligence unit within the National Crime Agency (NCA). NCA was created on 3 April 2006 by the Serious Organised and Police Act 2005. It is a law enforcement body devoted to dealing with organised crime within the UK and networking with other law enforcement agencies to combat global organised crime. For full details on NCA and their activities view their website at: http://www.nationalcrimeagency.gov.uk/

A defence (consent)

It is an offence for the nominated officer to proceed with a transaction prior to receiving a granted letter from the NCA within the 7 working day statutory time period". This period starts from the day after submitting the report.

A defence relates to offences in Proceeds of Crime Act and the Terrorism Act but not to other criminal offences.
Seeking a defence, granting it or no reply from the NCA is not a permission to proceed or oblige to proceed, nor is it an approval of an act or persons, or mean that there is no criminality involved. Company considers position carefully. A defence does not mean Company does not have to verify a customer's identity or that of any beneficial owners. The business must continue to comply with all the requirements of the Regulations.

If do not receive a refusal notification from the NCA within the notice period it is up to Company to interpret position. If Company considers that we have met the requirements for making a disclosure assume a defence.
If the NCA refuses a defence, must not proceed with a transaction for up to a further 31 calendar days, i.e. the moratorium period. In terrorist financing cases the moratorium period does not apply, do not have a defence until a request is granted.

The NCA has published information on obtaining a defence. Some of the key points include:

- a defence is only valid for the transaction reported - any future transactions by the same customer have to be considered on their own merits (and in the light of the suspicions that arose for the original one)
- can't ask for a general defence to trade with a customer, only to carry out a particular transaction
- the initial notice period is 7 working days from the date of the report; and if a defence is refused, the moratorium period is a further 31 calendar days from the date of refusal - if need a defence sooner, should clearly state the reasons for the urgency and perhaps contact the National Crime Agency to discuss the situation
- the National Crime Agency will contact by telephone and will confirm their decision in writing

STAFF AWARENESS AND TRAINING

General legal obligations

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 require businesses to take appropriate measures so that all relevant employees are:

- ensure relevant staff are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation, know who the nominated officer is and what his responsibilities are, train in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
- staff are trained at regular intervals
- maintain a written record of what have been done to raise awareness and the training given to staff
- ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

Who should be trained?

Employees should be trained in what they need to do to carry out their particular roles in the organisation. All customer-facing staff will require training in relation to recognising and handling suspicious transactions.

Nominated Officers/MLROs, senior managers and others involved in ongoing monitoring of business relationships and other internal control procedures will need different training, tailored to their particular functions.

What should training cover?

When consider who needs to be trained Company should include staff who deal with customers, deal with money or help with compliance. Think about reception staff, administration staff and finance staff, because they'll each have a different involvement in compliance, and have different training needs.

The training process should therefore cover the whole end to end process from sales and receiving customers' instructions, through to valuation, dealing with offers and completion.

Nominated officers, senior managers and anyone who is involved in monitoring business relationships and internal controls must also be fully familiar with the requirements of their role and understand how to meet those requirements.

Each member of staff should be ready to deal with the risks posed by their role. Their training should be good enough, and often enough, to keep their knowledge and skills up to date.

It should cover:

- the staff member's duties
- the risks posed to the business
- the business policies and procedures
- how to conduct customer due diligence and check customers' documents
- how to spot and deal with suspicious customers and activity
- how to make internal reports, including disclosures of suspicious activity
- data protection requirements
- record keeping
- the Money Laundering and Terrorist Financing (Amendment) Regulations 2019; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act

Training may include:

- face-to-face training
- online training sessions
- HMRC webinars
- taking part in special meetings to discuss the business procedures
- reading publications
- meetings to look at the issues and risks

A policy manual is useful to raise staff awareness and for reference between training sessions. Staff training is necessary when staff join the business, move to a new job or when they change roles. They should also have ongoing training at least every 2 years or when a significant change happens, depending on the level of risks.

Company must keep evidence of assessment of training needs and the steps we've taken to meet those needs. Company may be asked to produce training records in court.

Training records include:

- a copy of the training materials
- details of who provided training, if provided externally
- a list of staff who have completed training, with dates, and their signatures (confirming their understanding of the obligations) or electronic training records

- an updated training schedule

How often should training be given?

Businesses should ensure that the frequency of training is sufficient to maintain the knowledge and competence of staff to apply customer due diligence measures appropriately and in accordance with the business's risk assessments of the products or services they offer.

ALICO UK LIMITED gives training its entire staff every 12 months as part of ongoing staff training, to make staff aware of changing behaviour and practices amongst money launderers and those financing terrorism.

RECORD KEEPING

The purpose of The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 on record keeping is to require a business to be able to demonstrate its compliance with the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, through keeping evidence and records of due diligence checks made and information held on customers and transactions. These records may be crucial in any subsequent investigation by NCA, the police or HMRC. They will enable the business to produce a sound defence against any suspicion of involvement in money laundering or terrorist financing, or charges of failure to comply with the regulations.

The records that must be kept

The records that must be kept are:

- Copies of the evidence obtained of a customer's identity for five years after the end of the business relationship
- Details of customer transactions for five years from the date of the transaction
- Details of actions taken in respect of internal and external suspicion reports
- Details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make a suspicious activity report
- Copies of the evidence obtained if are relied on by another person to carry out customer due diligence, for five years from the date of the agreement, the agreement should be in writing

Company must also maintain:

- a written record of your risk assessment
- a written record of your policies, controls and procedure

Transaction and business relationship records (for example, account files, relevant business correspondence, daily log books, receipts, cheques, and so on) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

How long the customer due diligence records must be kept?

Company must keep records of customer due diligence checks and business transactions:

- for 5 years after the end of the business relationship
- for 5 years from the date an occasional transaction was completed
- should also keep supporting records for 5 years after the end of a business relationship

- should keep records from closed branches or agents

The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents is held.

Risk assessment and policies, controls and procedures must be kept up to date and be amended to reflect any changes in your business.

In what format must the records be kept?

Most businesses want to keep to a minimum the volume and density of records which need to be kept whilst still complying with the Regulations.

Records may therefore be kept:

- By way of original documents
- By way of good photocopies of original documents
- On microfiche
- In scanned form
- In computerised or electronic form.

After the period above the records can be deleted unless you are required to keep them in relation to legal or court proceedings, not be required to keep them for more than twenty five years.

All electronic records must be subject to regular and routine backup with off-site storage.

Penalties for failure to keep records

Where the record-keeping obligations under Money Laundering and Terrorist Financing (Amendment) Regulations 2019 are not observed, a business or person is open to financial penalties or potentially prosecution including imprisonment for up to 2 years.

SUSPICIOUS ACTIVITY REPORT FORM (INTERNAL)

SAR No: .....

Particulars	Remarks
Date:	
Id of the customer:	
Suspect:	
Name/address of Customer:	
Telephone no of Customer:	
Nature of suspicious activity:	

Give full detail of suspicion: [Include detail of transactions and identity checks.]	
Attach any relevant documents:	Yes/ No
Name of the Reporting Officer:	
Signature by Reporting Officer:	
Refer to NCA: [To be completed by MLRO]	Yes/ No
Do not refer to NCA: Reason for decision: Details	
Date referred to NCA:	

Approved By: .....

MLRO & Director

CERTIFICATE FOR DECLARATION OF CUSTOMER'S SOURCE OF FUND & PURPOSE OF USE.

[Required for all transactions in where source of funds are not adequate]

Employee's Name: _____ Date: _____

Amount to be transferred	One Off: £…… Linked: £……Period [From……. To……..]

Customer's Information:

Details	Remark [Fill the form or tick appropriate]
Name	
Occupation	
Type of Transaction	Bank/Online Transferred
Photo IDs and Proof of address Available?	Yes/No
Proof of Source of Income?***	Shown in Bank statement/Legal letter/Pay slips, …….[any other]
Verified the source of documents by Staff (tick)	Yes/No
Does the source of fund documents sufficient for remittance and/or Exchange?	Yes/No
Does Staff contacted with :	The Guarantor/solicitor/employer/ accountant Etc.
How Staff contacted to verify the source of documents with above parties?	Phone/email/face to face/……..[others]
Purpose of use abroad (by sender)***	
Proof of Purpose of Use, if Available	Found / Not Found

Source of Funds Declaration: hereby declare that I am not involved in any criminal or money laundering activity and the funds for the above transaction were obtained by me, are clear and are not derived from any illegal activities. These funds are derived from the following source:

Signature of Customer_____ Employee's Signature: _____

ONE-OFF TRANSACTION THRESHOLDS

Thresholds in GBP	ID Requirements
£1 to £3,000	1 Photo ID
£3,001 to £6,000	2 IDs (1 Photo ID & 1 Proof of Address)
£6,001 to £10,000	2 IDs (1 Photo ID & 1 Proof of Address) and Source of Fund documents
£10,001+	2IDs and Source of Fund documents and Declaration form EDD: Further information (Purpose of Sending, Profession and Calculate average Transaction of period)

LINKED TRANSACTION THRESHOLDS

Duration	Thresholds in GBP	ID Requirements
Rolling 90 Days Period	£ 1 to £ 3,000	1 Photo ID
	£ 3,001 to £6,000	2 IDs (1 Photo ID & 1 Proof of Address)
	£6,001 to £10,000	2 IDs (1 Photo ID & 1 Proof of Address) and Source of Funds
	£10,001+	2ID and Source of Fund documents and Declaration form EDD: Further information (Purpose of Sending, Profession and Calculate average Transaction of period)

Customer Information: Sender details: Full Name, current residential address, date of birth, Phone no, Receivers Details: full name, phone no, Relationship, Purpose of money sending.

1st form of ID: If only 1 form of ID (UK Full Driving License, Provisional License, Valid International Passport, British Passport, Asylum seeker Registration Card with work Permit).

2nd form of ID: UK Driving License, Provisional License, Posted Recent Bank Statement/Utility Bills of Gas/Electricity/Water/Council letter. (No Private company's bills or letter I.e. Phone Bills.)

Declaration of Fund: Self Declaration in specified Form from Company.

Source of Fund: Written documents showing the sale of legal asset, his/her pays lips/ Bank Statement that showing the income either salary, Sale of asset that matches or is near to the amount being transferred.

EDD: Further information:*Purpose of Use of the Fund: Any letter or Documents from firm/shop/lawyer/accountant/asset Buyer indicating the purpose and Use of Fund

Guidelines: FCA and HMRC ML Guidelines and Company MLR policy to be followed + Customer Due Diligence with every customer.