INSERT NAME OF THIRD PARTY SUPPLIER POLICY SUMMARY

LLOYDS BANKING GROUP	**Anti-Money Laundering and Counter Terrorist Financing** **SUMMARY FOR THIRD PARTY SUPPLIERS**

RATIONALE

Group Policy Rationale

This Policy has been designed to assist in managing the risk of Money Laundering, Terrorist Financing and the financing of the proliferation of weapons of mass destruction which are serious threats to security and the integrity of the financial system. The overall risk includes the following risk drivers:

- Failure to comply with legal and/or regulatory responsibilities in relation to Anti Money Laundering and Counter Terrorist Financing;
- Failure to deter and detect those who would seek to use the Group to facilitate the movement of criminal funds and funds designed to finance terrorism;
- Failure to prevent the facilitation of Tax Evasion.

In addition, this Policy has been designed to support compliance with the following legislation and / or regulations:

- Proceeds of Crime Act 2002;
- Anti-terrorism, Crime and Security Act 2001;
- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017;
- Counter Terrorism Act 2008;
- The Criminal Finances Act; and
- System and Control (SYSC) Rules of the FCA Handbook.

The Anti-Money Laundering & Counter Terrorist Financing Policy (the AML/CTF Policy) is a mandatory requirement for all businesses, divisions and legal entities within the Group and applies to all colleagues (temporary and permanent) in all jurisdictions in which the Group operates. The Policy clearly articulates a set of minimum standards and requirements that meet and often exceed UK regulatory and legislative obligations and the guidance provided by the Joint Money Laundering Steering Group (JMLSG).

Customer Impact

The Group's vision is to be the best bank for customers. The Groups Anti Money Laundering and Counter Terrorist Financing Policy (AML & CTF) supports this vision with the aim of providing investors with strong, stable and sustainable returns by helping to maintain the financial stability of the Group. The Policy also gives our investors and customers' confidence in the strength and integrity of the Group's compliance with legal and regulatory requirements. This is achieved by providing:

- Clarity on the Group's Anti Money Laundering and Counter Terrorist Financing Policy and risk appetite, ensuring that the Group minimises the

risk of its products, services or colleagues being used to launder the proceeds of crime, fund terrorism or facilitate Tax Evasion;
- Guidance on the risk-based training programme which allows colleagues to serve its customers in line with AML & CTF legislation, regulation and the Group's risk appetite; and

Guidance which allows Business Units to implement internal processes and controls including appropriate Customer Due Diligence, effective customer screening and transaction monitoring processes.

SCOPE

An external party supplying services to the Group or performing services on the Group's behalf will be expected to comply with the Group's AML/CTF Policy where those services form part of the Group's regulated activities.

In all other circumstances, this Policy is not applicable to third-party suppliers of goods or services to the Group.

Typical circumstances that **will** result in this Policy being applicable include the following services:

- On-boarding or introducing customers;
- Processing customer transactions;
- Providing the Group's financial products to customers; and
- Providing risk, compliance or audit services to the Group.

Typical circumstances that **will not** result in this Policy being applicable include:

- Providing goods to the Group;
- Performing services unrelated to the Group's regulated activities (e.g. security, transport, catering, printing, etc.); and
- Conducting activities outside the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing and Transfer of Funds Regulations 2017 (or equivalent).

MANDATORY REQUIREMENTS – GENERAL

- The supplier must comply with any anti-money laundering obligations to which they are subject in their own right, for example, by virtue of their falling within the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing and Transfer of Funds Regulations 2017 (or equivalent).

- The supplier must not engage in any conduct that results in it, or another party:

    - concealing, disguising, converting or transferring criminal property or terrorist funds;
    - entering into, or becoming concerned in an arrangement that facilitates the acquisition, retention, use or control of criminal property or terrorist funds; or
    - acquiring, using or possessing criminal property or terrorist funds.

- Where the Supplier is supplying a service to Lloyds Banking Group or performing a service on behalf of the Group that forms part of the Group's regulated activities and for which Lloyds Banking Group retains AML/CTF accountability, the Group will define for the supplier the specific requirements of the AML/CTF Policy relevant to that service. This may include some or all of the following:

    - Assessment of money laundering and terrorist financing risk;

INSERT NAME OF THIRD PARTY SUPPLIER POLICY SUMMARY

- Customer Due Diligence / Ongoing Customer Due Diligence (including forwarding CDD material upon request);
- Transaction Monitoring;
- Suspicious Activity Reporting;
- Responding to Court Orders;
- Provision of Management Information;
- Staff Training; and
- Record Keeping.

In all cases, Lloyds Banking Group will perform ongoing monitoring, oversight and assurance of the supplier's activities to ensure compliance with the AML/CTF Policy.

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Anti-Money Laundering & Counter Terrorist Financing Training Third Parties must ensure that all staff complete Anti Money Laundering and Counter Terrorist Finance (AML&CTF) Training at least annually.	1. AML/CTF training program in place. 2. Management Information: • Overall number of staff expected to complete annual training; • Number of staff who have completed annual training.	1. Annual review or any changes in applicable regulation/legislation. 2. Quarterly
Completion of New to Bank Customer Due Diligence (CDD) including Enhanced Customer Due Diligence (EDD) (where applicable) Third Parties must ensure CDD is in place to cover all aspects of CDD and EDD (including beneficial owners) in line with the requirements of prevailing Money Laundering Regulations.	1. Sample checking of New to Bank CDD records. 2. Management Information: • Number of accounts opened; • Number of accounts sampled; • Number of failures e.g. where the correct level of due diligence cannot be evidenced.	Monthly
Ongoing Customer Due Diligence (ODD) Third Parties must conduct ongoing monitoring of customer relationships to ensure existing records remain up to date.	1. Sample checking of ODD records. 2. Management Information: • Number of accounts subject to ODD review; • Number of ODD cases sampled;	Monthly

INSERT NAME OF THIRD PARTY SUPPLIER POLICY SUMMARY

	• Number of failures e.g. where completion of ODD cannot be evidenced or is incomplete.	
Politically Exposed Persons (PEPs) Third Parties must have appropriate systems and procedures to identify where a new or existing customer relationship (including beneficial owner) is a PEP.	1. Customer screening must be in place to identify PEP's at new to bank (NTB) or where an existing relationship may become categorised as a PEP. 2. Management information: • Number of PEP relationships identified.	1. Screening must be performed: • NTB within 24 hours; • Existing customers - daily screening. 2. Monthly.
Suspicious Activity Reporting (SAR) Third Parties must ensure that where knowledge or reasonable knowledge exists that a person has been engaged in money laundering or has identified that criminal/ terrorist property exists the Third Party must ensure that a suspicious activity report is made to the Lloyds Banking Groups (LBG) Nominated Officer.	1. Suspicious activity reports - Procedures must be in place that provides a mechanism for reporting internal suspicion when operating in the course of business. 2. Management Information: • Number of suspicious activity reports raised.	1. Procedures reviewed at least annually 2. Monthly.
Record Keeping Third Parties must ensure that requests for information relating to CDD including transactional data must be retained in accordance with prevailing regulation (Money Laundering Regulations 2017) and retrievable upon request within agreed timescales.	1. Procedures in place that ensure documentation is retained (whether physical or electronic) are accurate, legible and kept for an agreed period of time. It must include the mechanism for retrieval to agreed timescales. 2. Management information: • Number of instances where requests for information have not been met.	1. Procedures reviewed at least annually. 2. Monthly.

INSERT NAME OF THIRD PARTY SUPPLIER POLICY SUMMARY

Governance An individual must be appointed within the Third Party who has primary responsibility for the Anti Money Laundering and Counter Terrorist Finance control framework.	The appointed individual must ensure that: 1. Documented policies and procedures in relation to AML&CTF are maintained and meet regulatory and legislative obligations. 2. Management information is produced that provides details on levels of compliance and identifies where remedial action is required. Management information must include the level of compliance against the following: > Staff training; > CDD; > ODD; > PEPs; > SARs; > Record keeping. 3. An independent oversight and monitoring programme is in place; 4. Governance arrangements are in place that ensure the escalation of management information and results of oversight and monitoring programme to the Third Parties Senior Management and LBG (as agreed) allowing for the effective management of ML/TF risks in a timely manner.	1. Annual review or any change in applicable regulation / legislation. 2. Monthly.

INSERT NAME OF THIRD PARTY SUPPLIER POLICY SUMMARY

MANDATORY REQUIREMENTS – NON-COMPLIANCE
Any material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager. The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.

Version Number	Effective Date
1.0	14 August 2015
2.0	14 August 2015
3.0	30 September 2016
4.0	26 June 2017
5.0	28 September 2018
6.0 (No changes made to content as part of this refresh)	04 October 2019
7.0	04 May 2020
Next Planned Revision: November 2020	