GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

LLOYDS BANKING GROUP	**ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT** **SUMMARY FOR THIRD PARTY SUPPLIERS**

RATIONALE

Group Policy Rationale

The definition of fraud used in this Policy is derived from the criminal definition in the Fraud Act 2006 (UK). It is defined as "risk of acts of deception or omission intended for personal gain or to cause loss to another party by customers/clients, suppliers, third parties, or colleagues." This Policy covers all types of fraud perpetrated against the Group and/or its customers.

The objective of the Policy is to provide a consistent, proportionate and effective approach to economic crime risk management, with specific focus on the management of fraud risks, through a framework of core requirements.

This Policy has been designed to assist in managing the risk of acts of deception or omission intended for personal gain or to cause loss to another party by customers/clients, suppliers, third parties, or colleagues. The overall risk includes the following risk drivers:

- The risk that the organisation fails to deliver and discharge the appropriate accountability for fraud;
- The risk that the organisation fails to identify and mitigate fraud risks;
- The risk that the organisation fails to identify fraud events;
- The risk that the organisation fails to respond to suspected and/or actual fraud events; and
- The risk that the organisation fails to learn from suspected and/or actual fraud events.

This Policy defines the Group's requirements that its third-party suppliers must meet to ensure an appropriate and consistent approach to the management of economic crime risks. These requirements are informed by:

- Financial Conduct Authorities (FCA) 'Senior Management Arrangements, Systems and Controls' (SYSC);
- FCA Principles for Business (PRIN);
- The Second Payment Services Directive (PSD2);
- Securities Exchange Commission (SEC) and Commodities Future Trading Commission (CFTC) – Dodd Frank Act;
- Senior Managers Regime (SMR);
- Proceeds of Crime Act (POCA) 2002
- Fraud Act 2006; and

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

- Criminal Finances Act 2017

In jurisdictions where the local legislative and regulatory requirements exceed the requirements set out in this document, the Supplier must comply with any higher standards.

Customer Impact

The Group's vision is to be the Best Bank for Customers.

This Policy supports this vision and the aim of providing investors with strong, stable and sustainable returns.

SCOPE

This third-party version of the Policy applies to third-party suppliers where it has been identified that the Group Policy applies to the provision of their goods and/or services.

This third-party version of the Policy includes management of customer, external and internal fraud as defined below:

- Customer fraud covers instances of fraud in all customer segments and channels where the customer is persuaded to authorise a payment due to a false understanding of the circumstances in which the payment is being made.

- External fraud covers:
  - 1st Party Fraud – where the customer commits, or attempts to commit fraud through their accounts or products; and
  - 3rd Party Fraud – where a third-party (i.e. not our customer) uses our customer's details to commit, or attempt to commit fraud.

- Internal fraud covers:
  - Fraud committed by, or assisted by colleagues (permanent, temporary, contract or agency), suppliers (and employees of suppliers) and business introducers. This includes the intention to exploit an organisation's trust or legitimate access to their assets for unauthorised and/or illegitimate purposes; and
  - Aiding and abetting others through recklessness or wilful blindness, where colleagues are not actively involved in a deception, but recklessly or knowingly allow it to happen.

MANDATORY REQUIREMENTS – GENERAL

Where a third-party supplier conducts services on behalf of the Group, appropriate and proportionate controls must be in place to protect Group or customer assets from fraud.

Non-compliance with any mandatory element of this Policy must be reported to the Policy Owner where it will be discussed and agreed whether it constitutes a Policy breach and whether it should be reported officially as such.

The third-party supplier must ensure:

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

1. Fraud controls are operated across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. These controls must be appropriate and relevant to the type of business and proportionate to the fraud risk;
2. Sample checking is undertaken to ensure employees adhere to key fraud processes across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details of key fraud processes checked and all findings must be shared with the Group's supplier manager on request;
3. Ongoing control testing/assurance plans are in place to monitor the effectiveness of fraud controls across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details and results of fraud control effectiveness monitoring must be shared with the Group's supplier manager on request;
4. Effective compliance with this Policy, identifying where remediation is required and implementing agreed actions. This includes identification of fraud risks, changes in fraud risks, events, control failings and/or Policy breaches. Where these impact the Group or its customers, they must be reported promptly to the supplier manager or nominated Group contact and a full programme of remediation activity undertaken to resolve the breach. Details of findings in relation to compliance with this Policy must be shared with the Group's supplier manager proactively;
5. Detailed Root Cause Analysis (RCA) is undertaken upon the identification of a fraud event. The RCA should establish if any control principles were breached. Results and remediation plans must be shared with the Group's supplier manager proactively;
6. New employees complete their fraud training within 8 weeks of employment, and prior to undertaking any task that may impact the Group or its customers, e.g. amending/initiating payments, managing Group data, or handling Group cash;
7. Fraud training is completed by all employees on an annual basis, unless there are appropriate reasons for non-completion, e.g. Maternity Leave, or Long Term Sickness;
8. Regular MI on fraud training completion rates for all employees are recorded. This MI must be made available upon request by the Group's supplier manager; and
9. A documented Fraud Policy for all the control principles; PREVENT, DETECT, RESPOND AND REMEDIATE is in place, as detailed below.

Fraud Policy

Third party suppliers must document their approach to the following PREVENT, DETECT, RESPOND AND REMEDIATE principles in their own Fraud Policy. The approach must detail the systems, controls and processes that are operated to manage the risk of fraud.

The Fraud Policy must:

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

- Be proportionate to the fraud risk, as identified through a risk assessment exercise;
- Be appropriate and relevant for the type of business;
- Cover all types of fraud risk i.e. external, internal and customer fraud;
- Be reviewed regularly, at least annually, or upon changes to the systems, controls and/or processes to ensure they remain up-to-date;
- Be shared with the supplier manager on request;
- Document the controls operated in respect of the respond and remediate principles of this Policy, detailed below. This must specifically include the expected triggers, levels of accountability and responsibilities for action; and
- Document the reporting and escalation processes that must be followed upon discovery of a suspected or actual fraud, including when you advise the Group.

PREVENT

Suppliers must ensure fraud threats are identified and fraud risks are mitigated through maintaining effective systems, controls and processes, prior to establishing a relationship and during the lifecycle of that relationship.
The third-party supplier must operate controls in respect of the following where it is applicable to the supplier:

1. **ID Validation (IDV):** proving that someone, or a company, is who they say they are and reside where they say they do when we have no existing relationship with them. This must include compliance with the Pre-employment vetting check requirements detailed in the Group Colleague Policy Summary for Third Parties;
2. **Assessing Entities & Relationships:** ensuring that, once a person or company has been identified, the potential fraud risks are assessed before entering into a relationship with them and throughout the lifecycle of the relationship;
3. **Authentication:** ensuring controls are in place to minimise the risk of unauthorised access. All interactions must be scored based on the potential risk of interaction. Interactions involving the payment of funds will require a higher level of authentication. Further information can be sourced via the supplier manager;
4. **Data & Intelligence Sharing:** ensuring fraud risk data and intelligence is proactively shared between the Group and the third-party supplier;
5. **Preventing Internal Fraud:** ensuring effective controls are in place to prevent internal fraud, supporting the Group's zero appetite for internal fraud; and
6. **Education and Awareness:** ensuring the third-party supplier provides customers and employees with information, either face to face, online, via a web page or a variety of methods to help them in protecting themselves against fraud. This should include keeping customers and employees abreast of current fraud threats or scams and providing guidance on when and how to report fraud.

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

DETECT

Suppliers must ensure fraud events are effectively identified and managed through maintaining effective systems, controls and processes, during the lifecycle of that relationship.

The third-party supplier must operate controls in respect of the following where it is applicable to the supplier:

1. **Channel Protection:** ensuring that channels used to deliver products and services are resilient to fraud, for example the provision of Malware defenses on online service channels;
2. **Activity & Transaction Monitoring:** ensuring suspicious transactional activity is monitored and alerted; and
3. **Detecting Internal Fraud:** ensuring staff activity is monitored and all suspicious activity is alerted to the supplier manager.

RESPOND

Suppliers must ensure maintenance of a clear Fraud Policy enabling the third-party supplier to react to fraud and suspected fraud events when they occur.

The third-party supplier must operate controls in respect of the following where it is applicable to the supplier:

1. **Customer Vulnerability:** ensuring an appropriate response to customers identified as vulnerable;
2. **Duped and Scammed Customers:** ensuring an appropriate response to customers identified as victims of fraud;
3. **Support to Customers and employees:** ensuring customers and employees are aware of who they should contact in the event of fraud;
4. **Reporting Fraud Performance:** ensuring management information is made available in a timely manner to the supplier manager relating to customers impacted by fraud and fraud prevention activity;
5. **Regulatory and Media Requests:** ensuring any such incidents are referred to the supplier manager in a timely manner; and
6. **Recovery:** ensuring clear articulation of roles, responsibilities, processes and procedures to support the recovery of funds.

REMEDIATE

Suppliers must ensure appropriate corrective actions are undertaken and root cause analysis completed where appropriate to reduce the future impacts of fraud on both the Group and its customers. The third-party supplier must operate controls in respect of the following where it is applicable to the supplier:

1. **Reporting of Fraud Cases:** ensuring clear lines of responsibility for both the third-party supplier and the Group in managing and reporting fraud cases to ensure swift reporting of non-compliance, loss and control failings that could impact Group or customer assets;

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

2. **Root Cause Analysis:** ensuring processes are in place to undertake root cause analysis and to identify the point of compromise and point of exit; and
3. **Exit of Relationship:** ensuring processes are in place to respond to staff fraud events, including clear criteria for seeking employee dismissal.

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Process Adherence Third party suppliers must undertake sample checking to ensure employees adhere to key fraud processes across all the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details of key fraud processes checked and findings must be shared with the Group's supplier manager on request.	1. % of controls in place to manage process adherence, evidenced as effective. 2. Findings shared with the Group's supplier manager on request	Annual
Fraud Control Effectiveness Ongoing control testing/assurance plans must be in place to monitor the effectiveness of fraud controls across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details and results of fraud control effectiveness monitoring must be shared with the Group's supplier manager on request.	1. % of all controls reviewed for effectiveness, evidenced as effective. 2. Details and results shared with the Group's supplier manager on request	Annual
Fraud Risk Management Third party suppliers must monitor effective compliance with this Policy identifying where remediation is required and implementing agreed actions. This includes identification of fraud risks, changes in fraud risks, events, control failings and/or Policy breaches. Where these impact the Group or its customers, they must be reported promptly to the supplier manager or nominated Group contact and a full programme of remediation activity undertaken to resolve the breach. Details of findings in	1. % of all new fraud risks, changes in fraud risks, events, control failings and/or Policy breaches shared with the Group's supplier manager proactively.	Annual

relation to compliance with this Policy must be shared with the Group's supplier manager proactively.		
Fraud Event Root Cause Analysis Third party suppliers must undertake detailed Root Cause Analysis (RCA) upon the identification of a fraud event. The RCA should establish if any control principles were breached. Results and remediation plans must be shared with the Group's supplier manager proactively.	1. % of RCA results and remediation plans shared with the Group's supplier manager proactively.	Annual
Fraud Training Third-Party Suppliers must ensure that all staff (new and existing staff) complete Fraud Training.	1. Fraud training program in place. 2. Management information: • Overall number of staff expected to complete annual training; • Number of staff who have completed annual training; • Number of new staff expected to complete training before undertaking any activity on behalf of the Group; • Number of new staff who have completed training before undertaking any activity on behalf of the Group; • Ensure evidence is available upon request by the Group supplier manager.	1. Annual review or any changes in appliable regulation/ legislation. 2. Quarterly.
Documented Fraud Policy Third party suppliers must document their approach to the PREVENT, DETECT, RESPOND and REMEDIATE principles in their Fraud Policy. The approach must detail the systems, controls and processes that are operated to manage the risk of fraud.	1. Have a documented Fraud Policy in place. 2. Shared with the Group's supplier manager on request. 3. Ensure Fraud Policy reviewed and approved within last 12 months.	Annual

GROUP ECONOMIC CRIME PREVENTION POLICY – FRAUD RISK MANAGEMENT

MANDATORY REQUIREMENTS – NON-COMPLIANCE
Any material differences between the requirements set out above and the supplier's own controls must be raised by the supplier with the 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 a way forward.

Version Number	Effective Date
1.0 Final	April 2014
2.0 Final	November 2015
3.0 Draft	October 2016
4.0 Final	September 2017
5.0 Final	August 2018
6.0 Final	April 2019
7.0 Final	May 2020
7.1 Fit For Purpose	June 2020
8.0 Final	24th May 2021
Next Planned Revision: May 2022	