GROUP PAYMENT SERVICES POLICY – SUPPLIER VERSION

SUMMARY FOR THIRD PARTY SUPPLIERS

RATIONALE

Group Policy Rationale

This Policy has been designed to assist in managing the risk that the Group fails to comply with payment legislation, regulations and scheme requirements as they apply to its payment operations and systems. This may result in poor customer service, regulatory censure and reputational damage. The overall risk includes the following risk drivers:

- Increased and complex regulation and legislation
- Increased competition and market disruption through rapid innovation

The Group Payment Services Policy ensures that the expectations of our customers are met when it comes to their transactional and service needs by ensuring that Lloyds Banking Group (the Group) is in control of payment services no matter where in the world they are initiated, processed or settled.

The payments environment is becoming increasingly regulated with rapid innovation in the ways in which customers want their payment services. Our objective is to ensure that payment services and systems are operated and developed in a way that promotes; the interests of our customers, effective competition in the marketplace and innovation.

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

- Payment Services Regulations 2017 (PSRs)
- Funds Transfer Regulation 2015
- Single Euro Payments Area (SEPA) Regulations

Business units outside the UK but within the EEA must adhere to the local legislation implemented under the Payment Services Directive (Directive 2015/2366 EC on Payment services in the Internal Market).

Customer Impact

The Group's vision is to be the best bank for customers. The Payment Services Policy supports this vision and the aim of providing investors with strong, stable and sustainable returns by:

- Creating a framework, based on the relevant payments regulations, to protect and provide a consistently fair outcome for our customers.
- Ensuring business units are aware of their obligations when managing payment services as part of their day to day activities.

- Ensuring all systems which support the activities in scope of the Payment Services Policy maintains integrity, provides trust, and a fair service to the Groups customers.

SCOPE

This third party version of the Policy applies to suppliers (also referred as Third Parties), where it has been identified that the Group Policy applies to the provision of their goods and or services, in relation to any part of the end to end payment services process on behalf of the Group.

Businesses operating outside the UK must ensure that local Country and Jurisdictional legislation and/or regulatory requirements are adopted in addition to the requirements of this Policy.

Where Policy requirements conflict, this must be documented within the annual attestation. Local laws or regulations must take precedence.

Where this Policy has a requirement greater than local legislation, the Policy takes precedence.

This Policy uses the definition of a 'payment service' as defined under Schedule One of The Payment Service Regulation and FCA Approach Document;

Ref	Description	Examples
a	Services enabling cash to be placed on a payment account and all of the operations required for operating a payment account	depositing cash on a payment account (Including bulk cash collections, and deposits within mobile vans) ATMS, IDMs
b	Services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account	Withdrawing cash on a payment account (Including bulk cash collections, and deposits within mobile vans) ATMS, IDMs
c	The execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or another payment service provider- • execution of direct debits, including one-off direct debits; • execution of payment transactions through a payment card or a similar device; • execution of credit transfers, including standing orders	Execution of payments such as direct debits, standing orders, Faster Payments, CHAPs, BACS or debit cards.
d	The execution of payment transactions where the funds are covered by a credit line for the payment user- • execution of direct debits, including one-off direct debits; • execution of payment transactions through a payment card or a similar device;	Execution of payments such as direct debits standing orders, Faster Payments CHAPs, BACs etc. through a credit line (Overdrafts, credit cards)

	• execution of credit transfers, including standing orders	
e	Issuing payment instruments or acquiring payment transactions	Debit or credit cards, merchant transactions through a merchant acquirer such as Cardnet
f	Money Remittance	A service for the transmission of money (or any representation of monetary value), without any *payment accounts* being created for transferring - such as western union
g	Payment Initiation Service Providers	Where the Group has out sourced the process in initiating payments for customers who bank with different payment providers
h	Account Information Service Providers	Where the Group has outsourced the process to provide an aggregation of transactional account information on accounts held by the customer with different payment providers

Out of Scope;

- Relationships with third party banks.
- Third party-developed tools (e.g. Payments Systems, platforms) that are either fully hosted by the Group, or fully operated by Groups colleagues, and no operational payments processing is undertaken by the supplier on the Group's behalf.
- Business areas who are payment service users and have outsourced their payment processes.
  Business areas who are making non-customer payments such as colleague's salaries, maintenance building costs etc.

The Group Payments Policy Supplier Version Requirements are as follows:

1.1 POLICY AND REGULATORY ENVIRONMENT

a) Where this Policy has a requirement greater than local law, all parties must adhere to this Policy.
b) Where local legislation, including court orders, contradicts the Policy, local legislation takes precedence. Any instances of this must be documented in the annual attestation.
c) All parties must adhere to Payment Scheme membership rules and regulations, where a party is a member.
d) All suppliers must consider whether they are in scope for the Funds Transfer Regulation 2015. Where a party determines that they are in scope, they must ensure compliance to the relevant requirements, this includes the European Banking Authority's (EBA) guidelines under Article 25 of Regulation EU 2015/847. This includes full originator information and required beneficiary information in all fund transfers and related messages or instructions created on behalf of the Group's customers or the Group. Where it is available full beneficiary address should also be included. This information must remain throughout the Payment chain.
e) All suppliers must review the SEPA Regulation (EU260/12) and consider whether they are in scope. Where a party determines that they are in scope, they must ensure compliance to relevant requirements.
f) All suppliers must consider whether they are in scope of the Payment Services Regulations 2017. Where a party determines that they are in scope, they must ensure compliance to relevant requirements.
g) All suppliers providing a Payment Initiation Service or Account Information Service on behalf of the Group are required to transmit personalised security credentials through safe and efficient channels in accordance with Payment Services Regulations 2017.

1.2 PAYMENT INSTRUCTIONS

a) The customer must be identified through a process which proves that an individual or an entity is who they say they are and reside where they say they do before a customer instruction is processed.
b) Evidence that the checks in 1.2a have been completed must be maintained. A full audit trail must be maintained to evidence that all the necessary checks have been completed.
c) The customer's instruction must comply with the product or account authority/mandate and any other authorities or procedures applicable to the account.
d) For payments initiated, or processed in any other way, by the third party on behalf of the Group and not by a customer instruction, processes must be in place to ensure that the payment is being made to a known Third Party and is not fraudulent.
e) Under no circumstances must information in a payment instruction be omitted, deleted or altered; both manual processes and systems must be designed to prevent this from happening.
f) All payments are to be made in line with the appropriate authentication requirements. Please see the Group Fraud Risk Management Policy Summary for Third Party Suppliers here.

1.3 PROCESSING A PAYMENT INSTRUCTION

Payments Processing is defined as steps in the process of moving of funds from an originator's account to the beneficiary's account in a timely manner and in accordance with the customer's instructions. Such processing includes the receipt or creation of a payment instruction, the validation process, the processing of the payment instruction which includes any associated repairs required, processing of returned payments and the quality assurance and checking processes. There must be procedures in place to demonstrate that;

a) A full audit trail must be maintained of the payments processes performed by the Third Party on behalf of the Group.
b) In respect of each payment, all parties must meet at least one of the following before a payment is made:
    i. Segregation of duties (also known as four or six eye scrutiny) and/or dual control between the input, check and release of payments must be in place.
    ii. Where segregation of duties or dual control under i. (above) is not possible the business must have a documented process post payment control and quality checking that is at least as robust as segregation of duties and fulfils the same aim. Quality checking, dip testing and/or monitoring must be undertaken based on a statistically significant volume of payments.
c) All parties must give colleagues documented parameters for the types of work they are authorised to complete; for example, release payments up to a certain value. Controls must be in place to ensure adherence.
d) All parties must define and document their risk based approach for checking and identifying fraud. Controls must be in place to ensure adherence.
e) Under no circumstances must information in a payment instruction be omitted, deleted or altered; both manual processes and systems must be designed to prevent this from happening.
f) All parties who are involved in the receipt, creation or processing of a payment instruction must ensure that full originator information and required beneficiary information must be included in payment transfers and related messages. This information must remain throughout the payment chain.
g) Where a payment requires repair, documented processes must be in place and the repaired instruction must be treated as a new request and be checked appropriately.

1.4 PAYMENT ROUTING

The majority of financial messages, including payment instructions for cross border and domestic payments, use and follow the SWIFT standards and formatting. SWIFT is often used by countries as the transmission vehicle for local payment schemes. Therefore all parties must;

i. Use SWIFT when routing any payment instruction, ensuring it is used with the appropriate authenticated message type.
ii. Only channels which protect the integrity and confidentiality of the payment instruction or data may be used.

1.5 RECONCILIATION AND REPORTING

This sub-standard is applicable to Third Parties who conduct operational reconciliation activities on behalf of the Group for Sort Codes that are able to execute a payment linking to the systems listed below:

- CBS-Wholesale, Retail and Commercial Currencies
- Centralised Accounting Project -CAP
- NCA – New Current Account
- Common System
- TD01
- T24 & OCEAN (Islands Wealth Systems

a) All operational accounts must form part of an account landscape which is clearly documented, and validated and evidences key ownership and accountability
b) Every account that is reconciled must have a defined usage description and documented account matching criteria, write off limits and exception handling and loss sign off procedures.
c) A documented monitoring process must be in place to ensure operational reconciliation routines exist and are followed by all colleagues completing the reconciliation, and that colleagues undertaking account reconciliation are competent to do so. Evidence of monitoring having taken place must be maintained.
d) Aged analysis must take place on each account to ensure the control of older, outstanding items remain within appropriate risk appetite.
e) If parties are required to complete specific reporting of financial information on account balances, either internally or to external bodies, these requirements must be clearly documented and adherence evidenced.

1.6 INCIDENT REPORTING

In addition to their accountabilities under the **GROUP RESILIENCE & CONTINUITY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS,** suppliers must also be aware of the reporting requirements under the Payment Service Regulations 99 and the corresponding European Banking Authority's (EBA) guidelines under Article 25 of Regulation EU 2015/847. Suppliers should contact the Group immediately in the event that a qualifying incident has occurred so that timely reporting requirements to the FCA are met. Please see the Group Resilience & Continuity Policy (Including Incident Management) Summary for Third Party Suppliers, specifically the Incident Response (IR) section here.

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 inform the non-compliance to the Accountable Executive and Nominated Payments Officer for the relationship, and it will be the responsibility of the Nominated Payments Officer to consult their local Risk team to agree a way forward.

The Payments Officer is then responsible for raising the non-compliance through the waiver and breach processes outlined in the Group Payment Services Policy document.

Please see the Group Payment Services Supplier Version Attestation form embedded in the appendix section below. This needs to be completed as and when requested by the Payment Services Policy team, which is likely to be once a year. The usual approach for commencing this work is the Policy team reaching out to Nominated Payments Officers, with each business unit then working collaboratively with the supplier manager and supplier to complete the attestation.

APPENDICIES

Appendix A – Attestation Document

Payment Services Policy Supplier Attesta

Version Number	Effective Date
FINAL v1.0	01/04/2014
2.0	26/10/2015
3.0	05/08/2016
4.0	18/10/2017
5.0	02/03/2018
5.1	29/06/2018
5.2	25/10/2018
5.3	11/11/2019
5.4	15/04/2020
Next Planned Revision: October 2020	