Group Payment Transparency Procedures

Version Number	Version 2
Reference Number	PRFCGP001-015
Risk Control Area	Operational – Regulatory Compliance
Business Scope	Organisation Wide
Geographic Scope	Global
Status	Updated
Effective Date	31st January 2018
Related Policies	Group Anti-Money Laundering and Counter Terrorist Financing Policy

Owner: Rob Coombes
Head, FCC, CIB, CB, CRF and PRF, FCC C&I Clients & Products

Table of Contents

Version Control Table

Name	Changes Made	Approved by	Version Number	Date
Kriti Jain	Review and update Group Wire Transfer Procedures to Group Payment Transparency Procedures to include: • permitted exceptions to the Group Payment Transparency Procedures; • roles and responsibilities to enable compliance with relevant laws and regulations and consistent group wide execution; • information requirement: Emphasis on originator address to contain the country; • pre-condition of making wire transfers - identification of originator/beneficiary information in accordance with Standard Chartered Bank's Client Due Diligence Procedures; • detailed guidance on what constitutes Relevant Information Requirements in a wire transfer where Standard Chartered Bank is the originating Financial Institution; • the risk-based approach for execution/rejection of wire transfers or related messages; and • steps to detect and seek missing information and obligations regarding responding to information request.	Rob Coombes	2.0	31st Jan 2018

1. PURPOSE AND SCOPE

1.1. Purpose

The purpose of the Group Payment Transparency Procedures (hereafter may also be referred to as "Procedures" or "GPTP") is to provide minimum standards in relation to all electronic payments ("wire transfer") passing through Standard Chartered ("the Group") and/or its affiliates, and to manage and mitigate the risk of the Group being involved with wire transfers connected to Money Laundering and Terrorist Financing (collectively referred to as "ML"). The Group is committed to meeting its obligations in respect of wire transfers under relevant laws and regulation (please refer Section 1.2).

Payment Transparency means identifying and obtaining Relevant Information Requirements[1] on the underlying originator and beneficiary as well as any intermediary Financial Institution ("FI") in a wire transfers and passing this information in an accurate and meaningful manner through the payment chain as detailed in these Procedures.

Payment Transparency aims to facilitate full traceability, monitoring and sanction screening of wire transfers. Accordingly, these Procedures must be read in conjunction with relevant FCC policies and procedures covering Sanctions and ML.

This document replaces the Group Wire Transfer Procedures, which has been retired. All related Group documents referring to Group Wire Transfer Procedures shall be deemed as referencing to the GPTP.

All Group Offices are to ensure that their payment systems, channels, procedures and processes comply with requirements set out in these Procedures as well as their local laws and regulations.

1.2. Relevant Laws and Regulations

Financial Action Task Force ("FATF") Recommendation 16 (Wire Transfers) was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers to move funds, and to detect such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

- to appropriate law enforcement authorities;
- to financial intelligence units for analysing suspicious or unusual activity; and
- to Payment Service Providers ("PSPs") to facilitate the identification and reporting of suspicious transactions and complying with measures for combating money laundering and terrorist financing.

When setting these Procedures, the Group has taken into account relevant legal and regulatory requirements as updated from time to time, including the following standards:

- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017;
- the UK Joint Money Laundering Steering Group ("JMLSG") Guidance published June 2017 – Part III;
- FATF Recommendation 16;
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds ("Regulation 2015/847"). Regulation 2015/847 sets out rules on the information on payers and payees, accompanying transfers of funds, in any currency, for the purposes of preventing,

[1] Please refer to Section 3 for details on Relevant Information Requirements

detecting and investigating money laundering and terrorist financing, where at least one of the payment service providers involved in the transfer of funds is established in the European Union; and

- the Wolfsberg Payment Transparency Standards 2017 which requires FIs to implement the following four standards:
  - FIs should not omit, delete or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other FI in the payment process;
  - FIs should not use any particular payment message for the purpose of avoiding detection of information by any other FI in the payment process;
  - subject to applicable laws, FIs should cooperate as fully as practicable with other FIs in the payment process when requested to provide information about the parties involved;
  - FIs should strongly encourage their Correspondent Banks to observe these principles; and
  - it further gives guidance on payments messages, type of information that should be included, clarifies roles and responsibilities and expectations on originators, e.g. what it means to include name, address and account number. The standards also set out expectations on intermediary and beneficiary FIs, On Behalf Of ("OBO") payments and Money or Value Transfer Services ("MVTS") in relation to Payment Transparency.

1.3. Scope of Procedures

These Procedures apply to all cross border and domestic wire transfers, all currencies, all wire transfers carried out by electronic means between FIs; and all payment channels and units processing wire transfers either as originating/ordering, intermediary or beneficiary FIs involving the Group.

1.3.1. Permitted Exceptions

These Procedures are not intended to cover the following types of payments:

- where both the originating and beneficiary FI are acting on their own behalf, these are exempted from the Relevant Information Requirements, such as:
  - i) inter-FI settlements under MT200/202;
  - ii) cases where it is permitted to use unique identifier codes such as Business Identifier Code ("BIC") where it is sufficient to identify the client without full name and address information; and
  - iii) settlement of trade finance obligations under MT400 and MT700 series when they are used to settle trade finance obligations between Banks;
- message types and instructions that do not facilitate transfer of funds;
- Automated Teller Machines ("ATM") cash withdrawals where a client withdraws cash from their account;
- transfers of funds carried out through cheque images exchanges, including truncated cheques, or bills of exchange;
- paper based credit clearing systems such as UK credit clearing system as it is paper based; transfers carried out through paper based instruments (See Annex B for the scope of services under this exception); and
- over the counter cash and cheque deposits via Bank giro credits (Bank pay in slips).

2. ROLES AND RESPONSIBILITES STANDARDS

2.1. Avoidance and Circumvention

All staff must comply with the requirements of these Procedures and applicable laws and regulations within the scope of their direct organisational responsibilities.

No Staff may be involved in any manner in any activity intended to avoid or circumvent these Procedures. Any breach of these Procedures may, amongst other things, lead to disciplinary action and/or loss of employment. Any known non-adherence must be escalated to Country Money Laundering Compliance Officer ("CMLCO").

At no time, should any staff alter, modify or remove information from any wire transfer in an effort to mask a party in the wire transfer or use any message type that would impact the validity of the data or take any steps to avoid detection of information by any other FI in the payment process.

There may be a need to enrich wire transfer instructions received in order to facilitate more accurate and meaningful information. Enrichment for this purpose is permitted provided there is no underlying intention to avoid detection of information by applicable FIs or relevant authorities. Global Process Owners ("GPO") must set procedures to address these requirements.

2.2. Business and Function Level

The Business and Functions shall demonstrate that:

- their products, payment systems, channels, procedures and processes comply with these Procedures. They must implement and maintain such additional Department Operating Instructions ("DOIs") and guidance as required;
- product, platform and system used to effect a wire transfer:
  - i) do not restrict Payment Transparency by overwriting or deleting wire transfer information received in a wire transfer message;
  - ii) include details of originator and beneficiary and any intermediary FI used to transmit funds to ultimate beneficiary;
  - iii) allow for onward transmission of complete wire transfer information both within the Group and to third parties;
- where technical limitations exist and the Relevant Information Requirements accompanying a wire transfer cannot be passed due to its movement from cross border to domestic infrastructure (or domestic infrastructure to cross border), enrichment needed to repair payments to meet local regulatory requirements (please refer section 2.1) or any other infrastructure limitation; Group Offices must follow the guidance provided in section 5.5 and retain this information for at least 5 years or the period specified under applicable jurisdictional laws and regulations or Group Information Retention and Management Policy, whichever is greater. This information should be made available on request from other FIs in the payment chain;
- if an internal account (accounts owned by the Group) is used to process wire transfers OBO clients, the client information should be included in the wire transfer message. Routing of wire transfers through internal/suspense account should not result in wire transfer information being obscured;
- adequate engagement and education of clients and counterparties to ensure Group's expectation on Payment Transparency are well understood;
- dependencies on Client Due Diligence ("CDD"):

i) meeting the requirements of these Procedures, in many cases, rely upon the CDD information of the clients. Hence, Client Segment Heads or their relevant delegates must ensure that the client information is up to date in line with the Client Segment Client Due Diligence Procedures ("Group CDD Procedures") as listed in Annexure A; and

ii) furthermore, when giving clients access to Group's payment channels, consideration must be given on the need and purpose of these wire transfers and whether access is on a proprietary basis, or for the client's underlying customers or other third parties leading to OBO payments. Please refer to section 5.3 for further guidance on OBO payments.

2.3. Country Level

The CMLCO in each country is accountable for oversight and ensuring that the requirements of these Procedures are complied with at Country level.

The Group operates in many different jurisdictions and is therefore subject to different legal requirements and regulatory expectations in relation to wire transparency, and these Procedures set out minimum applicable requirements in relation to wire transparency which these jurisdictions must apply. The Group will comply with requirements set out in law or regulations and consider regulatory expectations in each country where it operates, where those requirements or expectations go beyond the standards of these Procedures. These requirements must be documented and adhered to within Country.

Where local requirements prohibit compliance with these Procedures, the CMLCO shall report the fact to the Global Head, Financial Crime Compliance ("FCC") or delegates; for any amendments as required, apply for a dispensation (see Section 12 for further guidance); and document requirements within appropriate Country Addendum, which may require Procedure Owner approval.

CMCLO is also responsible for assessing the need for any additional Procedures which may be required to meet local law and regulation and must seek approval for the additions from the Procedure Owner and document them within appropriate Country Addendum.

3. INFORMATION REQUIREMENT

All originator and beneficiary information requirements in these Procedures will be referred to as the "Relevant Information Requirements". These apply even where the originator and beneficiary hold accounts within the Group. These requirements are set out below.

3.1. Cross-border Wire Transfers

All cross-border wire transfers above USD1,000 or equivalent must consist of the following:

- Originator Information:
  - i) name of the originator;
  - ii) originator account number; and
  - iii) originator's address including country.
- Beneficiary Information:
  - i) name of the beneficiary;
  - ii) beneficiary account number where the funds are ultimately credited; and

iii) beneficiary country and address on best effort basis[2] at the time of wire transfer origination where the Group is the Originating FI.

All cross-border wire transfers below USD1,000 or equivalent must consist of the following:

- Originator Information:
  i) name of the originator;
  ii) originator account number;
- Beneficiary Information:
  i) name of the beneficiary; and
  ii) beneficiary account number.

Permitted exceptions under cross-border wire transfers:

- in the absence of account number, a unique transaction reference number must be included to enable traceability of the transaction; and
- in the absence of originator address, any of the following is permitted: a national identity number; or date and place of birth; or client/customer identification number[3]. This exception permitted for originator's address does not apply where the Group is the originating FI.

3.2. Domestic wire transfers

All domestic wire transfers must include the following originator information as indicated in cross border wire transfers:

- name of the originator;
- originator account number; and
- originator's address.

Where the above originator information cannot be carried forward due to domestic payment systems/schemes specified by local regulators/clearing houses not allowing full capture of the originator information or for any other reason, the Group as an Originating FI, need only include the account number or unique transaction reference number in the wire transfer, provided:

- this number or identifier will permit the transaction to be traced back to the originator or the beneficiary; and
- the originator information can be made available within three business days of receiving the request either from the beneficiary FI, intermediary FI or relevant authorities[4].
- No such obligations of checking originator information apply to the Group where the Group is the beneficiary FI, beyond what may be required by the local regulators/clearing houses on domestic payment pertaining to domestic wire transfers.

3.3. Payment Cards, Electronic Money Instruments, Mobile Phones, or any other Digital or IT Prepaid or Post-paid Devices with similar characteristics

Any transfer of funds that flows from a transaction carried out using a credit or debit or prepaid card (or any other digital or IT prepaid or post-paid device with similar

[2] Relevant GPOs and Channel owners to define good faith efforts to secure beneficiary country and address information as committed in SCB's response to the New York State Department of Financial Services Consent Order of August 19, 2014. The underlying objective being (i) increase the level of completeness of originator/beneficiary address (including country) information on affiliates; ii. encourage third parties (non-affiliates) to provide this information; and iii. implement an enhanced monitoring review protocol to apply where the above attempts fail.

[3] The customer identification number refers to a number which uniquely identifies the originator to the originating FI and is a different number from the unique transaction reference number. The customer identification number must refer to a record held by the originating FI which contains at least one of the following: the customer address, a national identity number, or a date and place of birth

[4] "Authorities" means, government, quasi-government, administrative, regulatory or supervisory body or authority or court or tribunal having jurisdiction over the Group

characteristics) for the purchase of goods or services, so long as the number of the card, instrument or device accompanies all transfers flowing from the transaction is exempted from the Relevant Information Requirements of this Procedure.

However, when a credit, debit or prepaid card (or any other digital or IT prepaid or post-paid device with similar characteristics) is used as a payment system to effect a person-to-person wire transfers, the transaction is covered by FATF Recommendation 16, and the Relevant Information Requirements must be included in the transfer of funds message.

4. PRE-CONDITIONS FOR MAKING WIRE TRANSFERS: VERIFICATION OF INFORMATION

Wire transfers above USD1,000 or equivalent (single or linked[5]) relating to the Group's clients must always carry verified Relevant Information Requirements. The verification requirement is deemed to be met ("verified") for Group's clients where the information obtained during their CDD review has been stored in accordance with the Group CDD Procedures.

Where the Group acts as an originating FI, the relevant GPOs must provide verified Relevant Information Requirements of the originator in the wire transfer message before transferring funds.

Where the Group acts as a beneficiary FI, the relevant GPOs must check the Relevant Information Requirements of the beneficiary against verified records before crediting the beneficiary's account or making the funds available to the beneficiary.

5. THE GROUP AS ORIGINATING FI (ALSO KNOWN AS ORDERING FI)

All Group Offices, acting as originating FI, must include the Relevant Information Requirements in every outgoing wire transfer. They must not execute the wire transfer where it does not comply with the Relevant Information Requirements specified in these Procedures.

Below is a detailed guidance on Relevant Information Requirements to be included when the Group is the ordering FI.

5.1. Originator Information

- Originator name (refers to the name of the client that has been verified):
  - i) clients that are natural persons, the name used must be the full name that was verified as part of CDD; and
  - ii) for clients that are legal entities (e.g. companies, partnerships) multiple names may exist such as registered legal name, trading name, 'doing business as' name or commonly abbreviated name. In the absence of any local regulations or client segment requirements, preference should be placed on legal registered name.
- Originator account number; and
- Originator address (refers to the client's address that was verified as part of CDD):
  - i) address information should be sufficient to clearly identify the location of the party(s) for screening and anti-money laundering ("AML") monitoring; and

[5] Where transfers appear to be linked to other wire transfers which together would exceed the USD1,000 or equivalent limit, the funds have been received or paid in cash or in anonymous electronic money, or where there are reasonable grounds for suspecting money laundering or terrorist financing

ii) it should include Country, and other aspects of an address in accordance with the resident country conventions such as City, State/Province/Municipality, Street Name, Building Number or Building Name, and Postal Code. Use of only a Post Office ("P.O.") Box as address should be avoided except where no alternative exists.

5.2. Beneficiary Information

- Name of the beneficiary: 'Name' refers to the name of the beneficiary as provided by the originator of the transaction and received by the Group Office. The name will not be subject to verification and the Group Offices should pass on the name as supplied by its client unless it is clearly meaningless. Examples of meaningless information include strings of random characters (e.g. 'xxxxx', or 'ABCDEFG') or terms such as 'our client', 'An Other', or 'My Customer'.
- Beneficiary account number: In the absence of an account number, a unique reference number must be included to enable traceability of the transaction.
- Beneficiary Address: 'Address' refers to the address of the beneficiary as provided by the originator of the transaction and should contain the country of the beneficiary on best effort basis[6]. The address however, will not be subject to verification and the Group should pass on the address as supplied by its client unless it is clearly meaningless.
- During processing, where the Group is aware that the beneficiary information does not contain the country of the beneficiary, the Group will, on best effort basis[7], obtain the information from the relevant party/parties.

5.3. On Behalf of Payments

On Behalf of Payments ("OBO") payments are when a client or Group's Internal Business Units are making wire transfers on behalf of an ultimate originator. In such cases the Group must ensure:

- Client Segments undertake sufficient due diligence on its clients at the stage of onboarding, assessing suitability to a product or periodic client reviews to confirm to a reasonable degree that wire transfers for third parties are consistent with the Group's understanding of the client's business; and
- Client Segments to ensure that their clients are enabled on tools that allow capturing of OBO information while initiating OBO payments and include full name and address details of the ultimate originator. The information of the ultimate originator need not be subject to verification and the Group should pass on the name and address as supplied by its client unless it is clearly meaningless.

Wire transfer messages must include the Relevant Information Requirement for the client and full name and address of the ultimate originator.

5.4. Cover Payments

The MT 202COV should be used for all outgoing cover payment transactions for which there is an associated MT103 and should replicate the information contained in the MT103 which complies with the Relevant Information Requirements. Alternatively, the 'serial MT103' method can be used in place of the MT 202COV method for sending client wire transfers.

MT202 should be used only for Bank to Bank transactions for their own purpose but must not be used to cover the funds related to an underlying client fund transfer.

[6] Refer footnote 2.

[7] Refer footnote 2.

5.5. Infrastructure limitations on field length and space

Where there are multiple account holders with different addresses, the verified address and name of the primary or first named account holder must take preference.

Address information should be provided in the fullest extent possible. Country or Country code is mandatory and where possible, followed by state/province/municipality, city and finally street and unit number. The above order is the order of priority to be followed when populating an address field constrained for length due to long names and addresses. It does not indicate the actual order in which the fields need to be populated in the address field.

For OBO payments, where both ultimate originator and client information cannot be provided in the same wire transfer, the information about the ultimate originator is more critical for anti-money laundering and counter terrorist financing purposes and must be disclosed in the wire transfer message. In this case, the Group must retain information on its clients and make this information available upon request from other FIs in the payment chain.

Relevant GPOs should set out guidelines to meet compliance with these Procedures on wire transfers generated and delivered from relevant Group's systems.

5.6. Enquiries on wire transfers where the Group is the originating FI

When a beneficiary FI or intermediary FI in any country requests a Group Office to provide the Relevant Information Requirements, that Group Office must:

- for any wire transfers that took place up to six months prior to the request, provide such information within seven working days of receiving the request; and
- as soon as practicable for any wire transfer that took place more than six months ago.

Where the enquiry is related to a domestic wire transfer that has been exempted from the Relevant Information Requirements, the Group is required to comply with the request within three business days of receiving the request.

6. THE GROUP AS INTERMEDIARY FI

Where the Group acts as Intermediary FI, it must ensure that all originator and beneficiary information received from the originating FI or another intermediary FI that accompanies a wire transfer is retained.

Following processing of the wire transfers, Group will adopt a risk-based sampling approach to identify wire transfers that do not comply with the Relevant Information Requirements. Where incoming wire transfers has been identified as non-compliant with Relevant Information Requirements, the Group must, post-transaction processing:

- seek the necessary information on the originator/beneficiary; and
- consider whether the meaningless or incomplete information constitute grounds for suspicion and escalation to FCC as per guidance in Section 9.

Enquiries on wire transfers where the Group is the intermediary FI: When a beneficiary (or Intermediary) FI in any country requests a Group Office to provide the Relevant Information Requirements, the Group Offices must within three working days provide the requesting FI with as much information as is in the Group's possession. The Group is not obliged under these Procedures to make requests to the originating FI on behalf of the beneficiary (or intermediary) FI, or to request the information from the originating FI for the Group's own records. A standard response to be sent to beneficiary or Intermediary FIs when the Group acts as an intermediary is attached to these Procedures. Please refer to Annexure C for Standard Messages.

7. THE GROUP AS BENEFICIARY FI (BENEFICIARY BANK)

Where the Group act as a beneficiary FI, it must ensure that all incoming wire transfers comply with the Relevant Information Requirements. Where incoming wire transfers have been identified as non-compliant with the Relevant Information Requirements, the Group must, post-transaction processing:

- seek the necessary Relevant Information Requirements on the originator/beneficiary; and
- consider whether the meaningless or incomplete information constitute grounds for suspicion and escalation to FCC as per guidance in Section 9.

8. RECORD KEEPING

All Group business units processing wire transfers must retain all necessary records on wire transfers, both domestic and cross-border, in accordance with Group Information Retention and Management Policy.

Such records must enable the reconstruction of individual transactions (including date of transaction, amounts and types of currency) to provide, if necessary, evidence for prosecution of criminal activity.

The records must evidence the verification of the identity of the originator and beneficiary in accordance with the requirements in the Groups CDD procedures.

9. MONITORING AND REPORTING

The Group's Data Owners (The Business Strategic Owner of a system supported by the respective Chief Information Officer[8]) that maintain the Relevant Information Requirements for transaction processing system to consume, need to ensure governance on data quality conforms with the responsibilities as stipulated in the Data Quality Management Policy and Procedures.

Downstream Process Owners to ensure that payment processing systems extract the verified Relevant Information Requirements from the Group's database and include the same in the wire transfer instruction. They must adhere to the responsibilities of 'Downstream Process Owner' as stipulated in the Group Data Quality Policy and Procedures;

The respective GPOs, who are responsible for products that generate wire transfers must set out effective procedures:

- to identify and report to FCC, in post transaction processing, USD wire transfers of USD 3,000 or more sent to or via the Group's New York office, where the Country of the originator or beneficiary cannot be determined;
- to meet obligations regarding responding to information requests from other FIs;
- to adhere to deadlines for remediating deficient transfers;
- to conduct periodic reviews as part of Operational Risk Framework ("ORF") and provide compliance to the usage of MT202/COV in place of MT202 for cover payments. Any MT202/MT202COV violations found as per these Procedures to be reported to the CBOC;

8 As defined in the Group Data Quality Policy and Procedures

- to detect wire transfers that lack or contain meaningless information leading to non-compliance of Relevant Information Requirements or inputs admissible in accordance with domestic payment systems/schemes specified by local regulators/clearing houses[9] and investigate and determine whether to query, reject or suspend such transfers of funds; and
- to detect such transfers, which are missing the Relevant Required Information including meaningless or incomplete information, the following steps should be taken:
  i) to seek missing information from the relevant originating or intermediary FI;
  ii) to determine whether to accept, reject, or suspend wire transfers that do not meet the Relevant Information Requirements;
  iii) to produce periodic reports that identify FIs that fail to comply with the requirements of these Procedures to local FCC Representatives.

Local FCC representatives must review these periodic reports received from respective GPO operational units to identify originating/intermediary FIs failing to provide the Relevant Required Information and provide the information to the relevant Regional FCC Correspondent Banking team for presentation, as deemed necessary, at the relevant Regional Correspondent Banking Oversight Group ("RCBOG") for review and determination on the appropriate course of action.

The relevant RCBOG:

- to have a risk based approach in establishing whether to issue warnings, setting of deadlines or placing restrictions before either rejecting any future transfers of funds from that originating/intermediary FI or recommending to terminate the, or part of, the relationship with the originating/intermediary FI;
- to escalate to the Correspondent Banking Oversight Committee ("CBOC") as appropriate and to seek CBOC approval before terminating the, or part of, the relationship with originating/intermediary FI; and
- report these failures, and the steps taken, to the CMLCO who will then assess and take the decision, if deemed necessary, to inform the relevant authorities responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

For all wire transfers in USD received by the Group's New York Office, FCC Americas Corporate Investment Banking Advisory/Regional Head FCC Europe and Americas will present enhanced reporting related to missing originator/beneficiary Country Information to the US Financial Crime Risk Committee ("USFCRC") for further action.

The Client Segment Groups must review those client relationships where it has been identified that the Relevant Information Requirements provided by the client is repeatedly (over a number of transactions and period of time) meaningless.

10. ASSURANCE

The Group will have an appropriate programme in place to monitor compliance with the Procedures across the three lines of defence in accordance with the Group's Risk Management Framework ("RMF"). The roles and responsibilities of the three lines of defence are documented in the RMF and the ORF.

9 See Section 3.2 for permitted exception under Domestic Wire Transfers

11. BREACHES AND RAISING CONCERNS

The Group and its Staff must not be involved in any activity intended to breach or circumvent any requirement set out in these Procedures. Willful or reckless breach or circumvention of these Procedures or applicable laws can have serious consequences for the Group, including criminal and civil fines, public censure and significant reputational and regulatory damage. Staff who circumvent these Procedures may also face criminal prosecution leading to imprisonment or fines, regulatory action and internal disciplinary action. If any client or counterparty is known or suspected of breaching (or attempting to breach) Procedure requirements, then the breach requirements set out in the Group Sanctions Policy and procedures and Group Anti-Money Laundering and Counter Terrorist Financing Policy should be followed as applicable. Concerns may also be raised with line managers, and the respective FCC Segment Team.

Any member of Staff who identifies a breach of this Procedure must report it immediately (where relevant with the assistance of their line manager) to their CMLCO. The CMLCO must analyse the information provided to them as a result of breaches or "Speaking Up" (as referred to in the Speaking Up Policy) and using their judgement, experience and expertise to determine whether the breach is sufficiently significant to be escalated to the respective Regional Head of FCC and/or Global Head, FCC. If they consider it necessary, Staff may use Speaking Up channels to make such a report rather than reporting directly to the CMLCO.

12. DISPENSATIONS

Procedure dispensations are time bound exemptions from whole or part of these Procedures. Dispensations from requirements to comply with these Procedures may be granted only in exceptional circumstances. Depending on the nature, applications for a dispensation must be:

- endorsed by one of the following:
  - i) Country Level: CORC or the equivalent committee, (or CFCRC where authorized and established to do so) where specific to a country;
  - ii) Business Segment/Product Level: Process Governance Committee ("PGC") where specific to a particular process; or
  - iii) Group Level: Relevant FCC Management Group Member;
- submitted in accordance with the Group approved Dispensation Template; and
- approved by the Policy Owner (or delegate).

Applications must be submitted to, reviewed by and approved by the Procedure Owner (or delegate). All dispensations and reasons for approving it must be recorded centrally on the RiskPod central register (unless not permitted by local legal requirements).

Information, guidance and templates around dispensations are contained in the Guidance for Publishing Dispensations on RiskPod document. RiskPod is the Group's central store for all dispensations, as well as, policies, procedures, committee terms of reference and glossary of key risk and control terms.

13. DEFINITIONS

Wire transfers / transfer of funds / Payments / Fund transfer	Any transaction, at least partially carried out by electronic means, on behalf of an originator through a payment service provider/FI with a view to make funds available to a beneficiary through a payment service provider/FI, irrespective of whether the originator and the beneficiary are the same person and /or have the same payment service provider/FI.
Person-to-person or peer-to-peer transfer of funds	Transaction between natural persons acting, as consumers, for purposes other than trade, business or profession.
Financial Institution (FI) / Payment service providers	Refers to any FI and non-Bank financial institution as defined in the Group's CDD Standards.
Originating FI / Ordering Bank / Payer PSP	Refers to the FI which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Intermediary FI / Intermediary Bank	Refers to FI in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering FI and the beneficiary FI, or another intermediary FI.
Beneficiary FI / Beneficiary Bank	Refers to the FI which receives the wire transfer from the ordering FI directly or through an intermediary FI and makes the funds available to the beneficiary.
Originator (Payer / Ordering party)	Refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering FI to perform the wire transfer.
Beneficiary (Payee):	Refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer. It will be the final recipient/party named in the transfer as the beneficiary of the funds (to be) transferred.
Cross-border wire transfers	Refers to any wire transfer where the ordering FI and beneficiary FI are located in different countries. This term also refers to any chain of wire transfer in which at least one of the FIs involved is in a different country. This also applies to book transfers.
Domestic wire transfers	Refers to any wire transfer where the ordering FI and beneficiary FI are located in the same country. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the wire transfer message may be located in another country. The term also refers to any chain of wire transfer that takes place entirely within the borders of the European Economic Area (EEA).
On Behalf Of (OBO) payments	This is a wire transfers where the Group's client initiating the wire transfer is not the ultimate originator (e.g. as part of a legal settlement, a law firm who is the customer of the FI, is making a wire transfer on behalf of its clients who is the ultimate originator).
Channel	A means by which a wire transfers is received or sent.
Cover payments	Refers to a wire transfer that combines a payment message sent directly by the ordering FI to the beneficiary FI with the routing of the funding instruction (the cover) from the ordering FI to the beneficiary FI through one or more intermediary FIs.
The Financial Action Task Force (FATF)	FATF is an intergovernmental body mandated to set standards and promote effective implementation of measures for combating money laundering and terrorist financing. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available: (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets; (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary; and (c) to ordering, intermediary and beneficiary FIs to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds considering the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.
Third party	Relating to a person or group besides the Group or a client of the Group.
Ultimate originator	Party on whose behalf the 'originator' is making a fund transfer. The originator is the holder of the account with the Group.
Unique transaction reference number	Means a combination of letters, numbers or symbols determined by the FI, in accordance with the protocols of the payment and settlement systems or messaging systems used for wire transfer, which permits the traceability of the transaction back to the originator and beneficiary.

14. PROCEDURE GOVERNANCE

Procedure Owner	Rob Coombes
Procedure Owner Job Title	Head, FCC, CIB, CB, CRF and PRF, FCC C&I Clients & Products
Inquiry Contact	Kriti Jain, Director, FCC Cash
Approving Party	Rob Coombes, Head, FCC, CIB, CB, CRF and PRF, FCC C&I Clients & Products
Approval Date	31st January 2018
Last Change Date	31st January 2018
Last Review Date	31st January 2018
Next Review Date	31st January 2020
Approver of Document Publishing	Yannick Cherel, Head, FCC Cash, Securities Services, Digitisation and Client Access

ANNEX A: RELATED DOCUMENTS

Documents that support the Group Payment Transparency Procedures:

- Client Segment Client Due Diligence Procedures[10]
    - Corporate and Institutional Banking/Commercial Clients CDD Procedures
    - Group CDD Procedures also known as "OneBank CDD Procedures"
    - Retail Business Banking Customer CDD Procedures
    - Retail Individual Customer CDD Procedures

Related Policies and Procedures:

- Group Anti-Money Laundering and Counter Terrorist Financing Policy
- Group Data Quality Policy and Procedures
- Group Information Retention and Management Policy
- Group Sanctions Policy & Procedures
- Group Speaking Up Policy
- Guidance for Publishing Dispensations on RiskPod

Related documents:

- Operational Risk Framework
- Risk Management Framework

ANNEX B: TRANSFERS CARRIED OUT THROUGH PAPER BASED SYSTEM

Payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the beneficiary:

- paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques;
- paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;
- paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;
- paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;
- paper-based vouchers;
- paper-based traveller's cheques; or
- paper-based postal money orders as defined by the Universal Postal Union.

ANNEX C: STANDARD MESSAGES

The standard messages for request of information ("RFI") as described in these Procedures are attached here:


Standard Message 1 First Request


StandardMessage2_ SecondRequest.doc


StandardMessage3_I ntermediaryResponse


Process for Responding to Other

[10] As updated from time to time by relevant Policy and Procedure Owners.