

CONFLICTS OF INTEREST POLICY SUMMARY

ICBC (Europe) S.A., Paris Branch

1. INTRODUCTION

In accordance with the applicable legal and regulatory framework, the Conflict of Interest Policy (hereinafter “the Policy”) of ICBC (Europe) S.A. Paris branch (hereinafter “the Bank”) sets out the framework enabling the prevention, identification, assessment, escalation, documentation, management and mitigation of actual and potential Conflict of Interest (hereinafter “COI”), including those that may arise in the context of MiFID related services; which potentially may affect the Bank’s ability to act with loyalty and integrity and could therefore damage the interest of the latter or its customers.

The purpose of this Policy is to:

- Define conflicts of interest and provide guidelines for the identification and management of situations/circumstances that may give rise to actual or potential conflicts of interests according to the activities carried out by the Bank
- Specify the organizational and procedural arrangements with the view to take all reasonable steps to prevent, escalate, document, manage and mitigate conflicts of interest

2. SCOPE OF APPLICATION

The Policy applies to ICBC (Europe) S.A. Paris branch.

DEFINITIONS

General

For the purposes of this policy, the following definitions apply:

Concept	Definitions
Authorized Management ("AM")	Means the member of the management body (at Headquarters and subsidiary institutions levels) in its management function, responsible for the effective, sound and prudent day-to-day management of business activities (and inherent risk) in compliance with the strategies and guiding principles laid down by the Board of Directors and the existing regulations, taking into account and safeguarding the Bank's long-term financial interests, solvency and liquidity situation.
(the) Bank	ICBC (Europe) S.A., Paris Branch
Customer	Natural or legal person with whom a business relationship exists with the Bank for the provisions of services or products, including persons acting or purporting to act on behalf of the customer. This may include existing or potential customers
Headquarter	ICBC (Europe) S.A in Luxembourg (hereafter "HQ")
Inside information	Information of a precise nature, which has not been made public, related - directly or indirectly - to (i) one or more issuers or (ii) one of more financial instruments, and which if made public, would be likely to have a significant effect on the prices of those financial instruments.
Internal control functions	The functions in charge of effectively managing the day-to-day operation of the independent risk management : Compliance, Permanent Control Department (PCD) and Internal audit of HQ
Third-Party Service Provider	External non-affiliated individual or entity providing services (e.g. consulting, legal, storage, processing, etc.) to the Bank. Any relationship with a Third-Party Service Provider that is governed by a Service Level Agreement.
Staff members	Staff members include - but is not limited to - all employees of the Bank, incl. Authorized Managers, consultants, temporary workers and agency workers (excluding third party suppliers such as cleaning and maintenance staff).

Conflict of interest

Under this policy, a conflict of interest (hereinafter “COI”) refers to a situation where the Bank, a Staff Member, a Customer or a third-party service provider has a vested interest which may be subject to an improper influence on decision-making processes or on the outcomes of the business or is not in the position to directly influence any decision-making or business. The Bank distinguishes:

- Actual Conflict of Interest (e.g. COI that has arisen); and
- Potential Conflict of Interest (e.g. COI that may arise due to specific circumstances).

COI may arise – but is not limited to – in the following variety of relationships, that are often closely related and may overlap:

- The Bank and a prospective/existing Customer (this also includes customer’s connected or related parties);
- The Bank and a Third-Party Representative;
- A Customer (or Group of Customers) and another Customer (or Group of Customers);
- A Customer (or Group of Customers) and a Staff Member;
- The Bank and a Staff Member;
- Entities of ICBC Group.

COI relating to Customer can be where the Bank, a Staff Member or a Third Party service provider¹ :

- is likely to make an inappropriate financial gain or avoid financial loss at the expense of a Customer;
- has an interest in the outcome of a service provided to a Customer or of a transaction carried out on behalf of a Customer which is different from the Customer’s interest in that outcome;
- has a financial or other incentive to favor the interest of a Customer or group of Customers over the interests of another Customer;
- carries on the same business as a Customer;
- receives or will receive from a person (other than the Customer) an inducement in relation to a service provided to the Customer, in the form of monies, goods or services, other than a standard commission or fee for that service;
- has a financial or other incentive to favor the sale of a particular product or service to a Customer which is not in the best interest of the Customer.

COI relating to the Bank can be broadly described as scenarios where, for example:

- A Staff Member (or where applicable, a family member or close personal relationship) receives a financial or other significant benefits as a result of the Staff Member’s

¹ Including his or her sustainability preferences

position at the Bank that could be inappropriate in nature

- A Staff Member's existing financial or other interest from previous engagement (endeavor, activity or relationship) with another person/employer, impairs or could impair his or her judgment or integrity in carrying out his or her duties and responsibilities to the Bank.

3. GENERAL PREVENTIVE MEASURES AGAINST CONFLICTS OF INTEREST

3.1. Implementation of effective policies and procedures

In order to prevent the occurrence of COI, the Bank has put in place an adequate framework and adopted effective policies and procedures.

In order to minimize the potential COI, the Bank has set up an appropriate segregation of duties and activities, including through the management of information access and the use of Chinese walls.

- **Segregation of duties and independence:** The Bank has implemented governance arrangements incorporating the three-line-of-defense model and taken appropriate measures to separate the decision-making process in order to ensure the independence and the proper management of actual or potential COI between the different business lines, with due regards to the Bank's and its customers' interests. Specific measures have been put in place to prevent or control the simultaneous or sequential involvement of staff to several services or activities where such involvement may impair the proper management of COI.
- **Information barriers (Chinese walls):** The Bank has established internal organizational arrangement to avoid COI by controlling, managing or restricting – as deemed appropriate – the flow of privileged information between the different areas of business or within a specific department or unit. Information barriers (both electronic and physical) are known as “Chinese walls” and are a key tool for the management of COI. Indeed, the Bank's main segregation divides its businesses into two categories: (i) the **public side**, with staff members who engage with investing customers on the basis of publicly available information only and (ii) **other departments** described as private side because they routinely receive or have access to “restricted information”². Indeed, “restricted information” for a particular transaction are to be shared between a small group of only those who really need the information to carry out their duties. This is usually the immediate 'deal team' as well as the internal control functions (Compliance, RMD and PCD) and AM members. Restricted information may only be passed between business areas in accordance with the “need-to-know” principle. In accordance with this approach, the Bank controls access to non-public information

² Restricted information includes both 1) inside information (intended as an information of a precise nature that, if made public, would significantly impact the price of related securities and 2) confidential information, incl. material which may not necessarily be price-sensitive and which may not obviously appear to be commercially sensitive.

through maintaining information barriers to prevent unauthorized access and misuse of non-public and inside information.

3.2. Self-limitation on services offered

When the Bank is already acting for one customer, there might be cases where it is inappropriate for the Bank to provide services to another customer, shall the Bank not be able to properly manage the COI. In such cases, the Bank will limit itself on the deal covered by the mandate, to avoid providing services which could harm one or more customer's interests.

3.3. Withdrawal / Decline to act

There might be circumstances where it is not appropriate for the Bank to continue to act for a customer or to be involved in a particular business relationship or arrangement (transaction, deal, agreement...), as it can be determined that the Bank is unable to effectively manage or prevent an actual or potential COI. In such circumstances, the Bank will need to withdraw from the proposed arrangement or business relationship. Also, in case of potential COI, if appropriate measures to manage the COI are considered insufficient or it may harm the customer's interest, the Bank will either decline to act for a customer or obtain the customer's consent in order to engage in an operation.

3.4. Other arrangements

Compliance function can also identify additional administrative and organizational arrangements to manage the COI. Compliance may also check that those measures have duly been included in the register and they have been implemented correctly effectively.

4. PROCEDURE AND CONTROL ARRANGEMENTS FOR THE MANAGEMENT OF CONFLICTS OF INTERESTS

4.1. Identification process

Staff members facing COI, have an obligation to report to Compliance.

Besides to the above obligation, when joining the Bank and then, on an annual basis, all Staff Members are required to confirm to Compliance receipt, reading and understanding of the Conflict of Interest Policy and if applicable, to declare any actual or potential COI.

Compliance shall, on a quarterly basis, monitor the status of potential and actual COI.

A mapping exercise aimed at identifying potential COI shall be carried out on a regular basis, and more particularly in the event of the providing of a new service/activity or a change in the Bank's organization.

4.2. Assessment process

Upon receipt of a notification of a potential or actual COI, Compliance shall analyze the circumstances and first determines whether or not it shall be qualified as a COI according to the factors and situations, and shall duly report the identified conflict with the associated assessment and recommendations to Authorized Management (AM), who shall decide on the

appropriate measures to be adopted for the best interests of the Bank and its customers. Compliance will document the decision taken, in particular, if the COI and related risks have been accepted.

All actual and potential COI should be adequately documented, communicated and discussed, decided on and duly managed by Paris branch. The Bank shall ensure that such cases will not impede the ability of members of AM to take objective and impartial decisions that aim to fulfill the best interests of the Bank, as well as its staff members, customer and other third parties.

4.3. Reporting

The Bank maintains a Conflict of Interest Register, where all potential and actual COI are logged as well as the compliance assessment, description of effective measures and acknowledgement of AM.

4.4. Disclosure to Customers

The Bank shall ensure that disclosure to Customers is a measure of last resort, upon approval from the AM, that shall be used only where the effective organizational and administrative arrangements established by the Bank to prevent or manage its COI are not sufficient to ensure, with reasonable confidence, that risks of damage to the interests of the customer will be prevented. The disclosure shall clearly state that the measures established by the Bank to prevent or manage that COI are not sufficient to ensure, with reasonable confidence, that the risks of damage to the interests of the Customer will be prevented.

5. DATA PROTECTION AND CONFIDENTIALITY

Within the framework of this Policy, the Bank stores and processes personal data of Staff Members and Third-Party Representative. In accordance with applicable laws and regulations on data protection (GDPR), the Bank only processes the data necessary for the implementation of this Policy.

It is ensured that the information disclosed regarding the actual or potential COI is protected, preventing access thereto by non-authorized staff members.

Information related to the Staff Member's COI is retained for five years from the date of the transaction took place or from the date the deal is finalized or the business relationship is closed.

6. TRAINING

The Bank shall ensure that adequate training and guidance is provided on a regular basis to all Staff Members on their obligations and on the applicable procedure concerning the management of COI.