

# Financial Crime Policy

27 April 2021

## 1. Objective

The objective of the Financial Crime Policy (“the Policy”) is to set out the principles for the management of risk and compliance associated with Money Laundering, Terrorist Financing, Sanctions, Bribery and Corruption, Fraud (internal and external), Tax Evasion and Facilitation of Tax Evasion in Danske Bank A/S (“the Group”).

The Policy is designed to ensure that the Group adheres to:

- Applicable laws and regulations in relation to Financial Crime compliance for the jurisdictions in which it operates; and
- Relevant Sanctions regimes in all jurisdictions in which it operates. These include European Union (“EU”), United Nations (“UN”), United Kingdom and any other applicable Sanctions as appropriate, as well as United States Sanctions to the extent they have extraterritorial application or risk implications for the Group’s business activities.

## 2. Definitions

The following definitions apply to the terms used throughout the Policy:

<b>Anything of Value</b>	<p>Anything a person might consider valuable, as Bribery occurs not only through the means of cash payments or financial transactions.</p> <p>Anything of Value can for example be a favourable hiring decision, access to an exclusive members-only club or tickets to an event.</p>
<b>Associated Person of the Group</b>	<p>Any natural person or legal entity, either incorporated or unincorporated, who performs services for or on behalf of the Group.</p> <p>All Employees are Associated Persons of the Group, as are suppliers, consultants, agents, intermediaries, introducers, brokers and business advisors. In addition, all Employees of joint ventures and consortia may also be Associated Persons of the Group, dependent on the nature of their relationship with the Group. This is not an exhaustive list.</p>
<b>Bribery</b>	<p>Bribery involves the offer, promise, request, acceptance or transfer of Anything of Value either directly or indirectly to or by an individual, in order to improperly induce, influence, or reward the performance of a function or an activity. An act of Bribery does not have to be successful for it to be considered a bribe. The Group considers Facilitation Payments to be Bribery as well.</p>

	<p>If an Employee of the Group is induced to make a decision or act in a certain way based on a benefit of any type received from a customer, Associated Person of the Group or Third Party, this may constitute criminal Bribery. Equally, if an Employee of the Group gives a benefit of any type in order to influence a decision or the behaviour of a colleague, customer, Associated Person of the Group or Third Party, this may also constitute criminal Bribery.</p>
<b>Business Unit</b>	<p>Business Unit shall be considered as the generic term to cover all first line businesses i.e. Personal &amp; Business Customers, Large Corporates &amp; Institutions and subsidiaries.</p>
<b>Close Associate of a Politically Exposed Person (“PEP”)</b>	<p>Known close associates of a PEP include:</p> <ul style="list-style-type: none"> <li>• a natural person who has joint beneficial ownership of a legal entity or legal arrangement with a PEP</li> <li>• a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP</li> <li>• a natural person who is able to conduct financial transactions on the PEP’s behalf</li> <li>• a natural person who, in other ways than those mentioned above, has a close business relationship with one or more PEPs</li> </ul> <p>Known close associates of a PEP are also considered a PEP.</p> <p>Further details of the definition can be found in the underlying instructions to the Policy.</p>
<b>Corruption Employee</b>	<p>Corruption is the abuse of entrusted power for private gain.</p> <p>For the purpose of the Policy, an Employee is considered to be:</p> <ul style="list-style-type: none"> <li>• A permanent or temporary Employee of the Group</li> <li>• A contingent worker, individuals who are working for the Group but are not directly employed by the Group (including officers, consultants, contractors, agency workers, etc.)</li> </ul>
<b>EU High Risk Third Country List</b>	<p>The EU High Risk Third Country List is published by the EU and includes those countries with strategic deficiencies in their national Anti-Money Laundering (“AML”) and Counter-Terrorist Financing (“CTF”) regimes that pose substantial threats to the EU and its financial system.</p>
<b>External Fraud</b>	<p>External Fraud should be considered as wrongful or unlawful deception intended to result in direct or indirect financial gain which is detrimental to the Group and/or its customers, which is committed or supported by external parties, including the Group’s customers.</p> <p>External Fraud can be categorised into:</p> <ul style="list-style-type: none"> <li>• First Party Fraud – where a customer misrepresents their identity, their financial intentions, or provide false information,</li> <li>• Third Party Fraud – where an external party has impersonated a customer without consent from the person whose identity is being used. This impersonation manifests</li> </ul>

	<p>itself in the creating of new accounts or in the takeover of existing bank facilities/products/services.</p> <ul style="list-style-type: none"> <li>• Authorised Push Payment Fraud (APP) - where a customer is deceived into making payments to either an incorrect beneficiary account (controlled by a fraudster) or where they have been deceived as to the nature of the goods and/or services they believe they will receive.</li> </ul>
<b>Facilitation Payments</b>	Facilitation Payments are payments or gifts made to Public Officials to hasten the performance of a routine action that are over and above the normal fee for that service or where a fee would not legally apply. For example, obtaining a visa at a border crossing.
<b>Facilitation of Tax Evasion</b>	Facilitation of Tax Evasion is when an Associated Person of the Group deliberately enables Tax Evasion.
<b>Financial Crime</b>	Financial Crime should be considered as the generic term for Money Laundering, Terrorist Financing, Sanctions, Bribery and Corruption, Fraud (both internal and external), Tax Evasion and Facilitation of Tax Evasion.
<b>Family Member of a Politically Exposed Person ("PEP")</b>	<p>Immediate family members of a PEP include:</p> <ul style="list-style-type: none"> <li>• spouse, civil partner, cohabitant or equivalent of that person</li> <li>• children of that person and their spouses, civil partners, cohabitants or equivalent</li> <li>• parents of that person</li> </ul>
<b>Incident of Bribery</b>	<p>Immediate family members of a PEP are also considered a PEP.</p> <p>Any act of Bribery for which the Group bears any level of responsibility. An Incident of Bribery as it relates to the Group can only occur through the actions of an Associated Person of the Group.</p>
<b>Internal Fraud</b>	Internal Fraud should be considered as wrongful and unlawful deception intended to result in direct or indirect financial gain which is detrimental to the Group and/or its customers, which is committed or supported by a party internal to the Group.
<b>Money Laundering</b>	Money Laundering is the generic term used to describe the process by which the original ownership and control of the proceeds of criminal conduct is disguised by making such proceeds appear to have derived from a legitimate source.
<b>Politically Exposed Person ("PEP")</b>	PEPs are natural persons who have, or have previously held, a high political profile, or a prominent public function. A more detailed definition can be found in the underlying instructions to the Policy.
<b>Public Official</b>	<p>A Public Official is considered to be a natural person in any rank or level at the following types of legal entities, organisations, and bodies:</p> <ul style="list-style-type: none"> <li>• national, regional, local or municipal governmental bodies (e.g. executive, legislative, judiciary)</li> <li>• state-owned or state-controlled legal entities or funds. Generally a legal entity would be deemed state-controlled where a government body has at least one of the following attributes: <ul style="list-style-type: none"> <li>○ more than 50% of ownership,</li> <li>○ voting control,</li> <li>○ board control, or</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ other indicia of control (e.g. golden share, government demonstration of control)</li> <li>● central banks</li> <li>● sovereign wealth funds</li> <li>● international organisations, development banks and public health agencies (e.g. the UN, EU, World Bank or International Monetary Fund), as well as mixed private-public entities (e.g. a cooperative arrangement between the public and private sector)</li> <li>● royal families</li> <li>● embassies and embassy diplomats.</li> <li>● political parties, party officials and candidates for any level of a political office.</li> </ul>
<b>Sanctions</b>	Sanctions are restrictions or prohibitions which are imposed by laws and regulations which can target economic, diplomatic, financial and trade activities with specific countries, governments, entities, organisations and/or individuals. Sanctions typically consist of asset freezes, travel restrictions, export and import restrictions, financial sanctions and other measures specified under a Sanctions program.
<b>Senior Management of the Group</b>	Senior Management of the Group constitute the members of the Board of Directors and the Executive Leadership Team.  When the Policy is adopted by a subsidiary, references to Senior Management should be understood as meaning the responsibilities undertaken by the management body of that subsidiary.
<b>Staff Areas</b>	Staff Areas should be considered as a generic term, which refers to and covers areas in the Group that have no ownership of any customer relationships such as CFO Area, Group Compliance Technology & Services, Group Risk Management, Group Legal, Group Human Resources ("HR"), Company Secretariat, Group Internal Audit and Group Communications, Brand & Marketing.
<b>Tax Evasion</b>	Tax Evasion is considered the act whereby liability to tax is deliberately concealed or ignored.
<b>Terrorist Financing</b>	Terrorist Financing is the provision or collection of funds with the intention that these funds can be used to carry out an act of terror, or be used to support any terrorist group, persons or associations in any ways.
<b>Third Party</b>	A Third Party is a legal entity, company, or person(s) that is not Danske Bank A/S or a Group entity of Danske Bank A/S.

### 3. Scope

The principles of the Policy set the Group's approach for Financial Crime risk management and compliance with Financial Crime related laws, regulations, regimes and other requirements that are applicable to the Group and its operations.

#### 3.1. Target Group

The Policy applies to all Employees in the Group and all subsidiaries as well as all Third Parties acting on behalf of the Group. All other Associated Persons of the Group must agree to comply with the Policy when acting on behalf of the Group.

The management body of a subsidiary may approve the Policy with deviations to ensure the policy is fit for purpose for the subsidiary. The policy administrator in the subsidiary should justify the rationale behind the deviation and ensure that the administrator of the Policy is consulted and endorses any deviation.

The administrator of the Policy must document and report any deviations from the Policy to the Executive Leadership Team of Danske Bank A/S. The Executive Leadership Team shall report all material deviations from Group Policies to the Board of Directors of Danske Bank A/S.

#### 3.2. Breaches

Lack of adherence to the Policy may have severe consequences to the Group and its Employees including:

- violating Financial Crime laws, regulations and regimes
- receiving monetary fines, criminal penalties, and/or regulatory enforcement orders
- exposing the Group to financial and customer risk and reputational risk

A breach is defined as non-compliance with any requirement in the Policy which has not been approved by the administrator of the Policy. All breaches must be reported to Group Compliance in accordance with applicable Group policies, including in particular the Escalation Policy and Whistleblowing Policy.

Lack of adherence to the Policy may also lead to disciplinary action up to and including potential dismissal, contract termination, criminal indictment or claim of damages.

## 4. Policy Content

### ***Principle 1: The Group must maintain a governance framework that clearly defines roles, accountabilities and responsibilities for Financial Crime compliance***

The Group must develop a governance framework that is promoted and maintained across all areas of the Group that includes:

- Clearly allocated accountabilities and responsibilities to manage Financial Crime risk;
- An appointed AML responsible member from the Executive Leadership Team, an AML Responsible Compliance Officer and an AML Responsible Person in the First Line of Defence;
- A strategy from Senior Management that actively promotes a strong Financial Crime compliance culture;
- Governance that sets out appropriate mandates, authorities and oversight capabilities; and
- Adequate resources in respect of personnel, competency and technology.

The governance framework must also include the specific accountabilities held by the relevant bodies and functions within the governance structure, including the Senior Management, Group Compliance and the Business Units.

### ***Principle 2: The Group must apply the Three Lines of Defence Model to ensure effective governance and oversight of Financial Crime risk***

The Group applies the Three Lines of Defence Model in accordance with the Group's Enterprise Risk Management approach. The Three Lines of Defence Model is a key element in ensuring effective governance and oversight of Financial Crime risk, including having clearly defined roles and responsibilities in place.

The Group's frontline units and their direct support functions within the Business Units constitute the **First Line of Defence** and are accountable for identifying, mitigating and managing Financial Crime risk associated with (but not limited to) customers, Third Parties, Associated Persons of the Group, products, and services. This includes designing, implementing and executing controls and processes to identify and manage Financial Crime risks within their business and operations, and performing ongoing oversight on the effectiveness of these controls and processes.

Group Compliance constitutes part of the **Second Line of Defence**. Group Compliance is responsible for ensuring the Group has adequate and robust policies and instructions addressing Financial Crime compliance, while also monitoring, testing, supporting, advising and challenging First Line of Defence risk management and compliance practices. Group Compliance is also responsible for conducting a risk assessment that identifies and measures the inherent risk of Financial Crime and evaluates the design and effectiveness of controls to determine the Group's residual risk.

Group Internal Audit constitutes the **Third Line of Defence**. The scope of Internal Audit's mandate is unrestricted and includes oversight of the activities conducted by both the First and Second Lines of Defence.

***Principle 3: Employees and other Associated Persons of the Group must not participate in misusing the Group's infrastructure, products and services for Financial Crime purposes***

All Employees and other Associated Persons of the Group are prohibited from, directly or indirectly, actively or passively advising on, facilitating, engaging or participating in activities or behaviour that misuse the Group's infrastructure, products and/or services for Financial Crime purposes or otherwise circumvent requirements imposed by the Policy and its underlying instructions.

Employees and other Associated Persons of the Group must not make Facilitation Payments as it relates to responsibilities associated with the Group, except in instances where the person being asked to make the payment believes that refusal would endanger their personal or another person's safety. Any payments made under such coercive circumstances must be reported to Group Compliance. Even if a Facilitation Payment is requested in a jurisdiction where it is culturally expected and not prohibited by law, the Group defines these payments as Bribery.

In addition, the Group must set out the responsibilities that all Employees and other Associated Persons of the Group have in the management of Financial Crime risk.

**Subprinciple 3.1: The Group must ensure that gifts, hospitality and entertainment are not used to engage in an incident of Financial Crime**

The Group must ensure that all Employees and other Associated Persons of the Group adhere to the Group requirements, thresholds and approvals for gifts and hospitalities before giving or receiving anything of value. This is regardless of whether it takes place during participation in external events or marketing events, roadshows or conferences held or sponsored by the Group which are attended by customers.

All gifts, hospitality and entertainment provided to or from customers or Third Parties must be in accordance with the Group's Gifts and Hospitality Instruction. Additionally, any conflicts of interest arising from the use of gifts, hospitality and entertainment must be reported in accordance with the Conflicts of Interest Policy.

**Subprinciple 3.2: The Group must maintain controls to manage the Financial Crime risk associated with its Employees and potential Employees**

The Group must ensure appropriate controls, where relevant and legally possible, are put in place to identify Employees engaging or participating in activities or behaviour that misuse the Group's infrastructure, products and/or services for Financial Crime purposes.

In addition, the Group must ensure that offers of employment are not used to engage in an incident of Financial Crime and where legally possible, that all potential Employees are screened in relation to Financial Crime risks (e.g. criminal records screening). All paid and unpaid (e.g. internships) employment must be agreed to and contracted through established standardised HR processes.

**Subprinciple 3.3: The Group must maintain controls to manage the Financial Crime risk associated with Employee incentives**

The Group must ensure that any incentives provided to Employees are not used to encourage an incident of Financial Crime.

All incentives must be agreed to and contracted through established standardised HR processes.

***Principle 4: The Group must have sufficient management information and reporting to monitor and oversee the management of Financial Crime risk***

The Group must develop and produce management information (“MI”), including both qualitative and quantitative key performance indicators and key risk indicators to maintain effective and meaningful oversight of the Group’s management of risk and compliance associated with Financial Crime and to inform Senior Management and other key stakeholders.

***Principle 5: The Group must apply a risk-based approach to ensure that risk mitigation measures are proportionate to the level of associated Financial Crime risk***

The Group must apply a holistic, risk-based approach to ensure that effective and appropriate controls are in place that are proportionate to the identified Financial Crime risk. The Group must identify and assess its Financial Crime risk to enable the effective design and implementation of adequate controls to manage and mitigate these risks in line with the Group’s Financial Crime risk tolerance and Group Non-Financial Risk tolerance statement.

In addition, applying a risk-based approach informed by a robust understanding of risk enables the Group to allocate and target its efforts and resources in the most efficient manner, with enhanced measures taken in instances that present an increased risk of Financial Crime.

***Subprinciple 5.1: The Group must conduct a risk assessment to identify and measure the inherent risk of Financial Crime and evaluate the design and effectiveness of controls to determine the Group’s residual risk***

The Group must complete a risk assessment, at least annually, that identifies and measures the Group’s inherent Financial Crime risk of and evaluates the design and effectiveness of controls to determine the Group’s residual Financial Crime risk.

The risk assessment must adequately account for the potential Financial Crime risk arising from all relevant factors, including (but not limited to) the Group’s customers, products, services, delivery channels, Third Parties, Associated Persons of the Group, transactions, technology and geographic locations. The risk assessment must also be proportionate to the size and complexity of the Group and its operations.

The risk assessment results must be used by the Group to inform the design, development, maintenance and implementation of the Group’s Financial Crime framework and other mitigation activities.

***Principle 6: The Group must maintain a control framework that enables effective and efficient mitigation of Financial Crime risk***

The Group’s internal control framework must identify, manage and mitigate Financial Crime risk. The framework must set clear expectations that include:

- Identifying, documenting and monitoring Financial Crime risk;
- Investigating and reporting potential Financial Crime incidents and violations;
- Defining and documenting risk-based control procedures and processes pertaining to Financial Crime compliance; and
- Regularly testing of the controls to ensure effective operation as well as ensuring the controls are appropriate and proportionate to the associated Financial Crime risk.

The framework includes screening, monitoring and due diligence controls that take into account relevant risk factors associated with customers, industries, geographies, typologies, products and service channels or a combination of these.



**Subprinciple 6.1: The Group must maintain controls to identify and manage the Financial Crime risk associated with its corporate development and strategic decisions**

The Group must ensure that any merger, acquisition, joint venture, principle finance investment or strategic decision to enter a new market, jurisdiction, product category or customer segment made by the Group considers Financial Crime risk as part of the due diligence, risk assessment, contracting, management and monitoring processes.

In addition, the Group must ensure that this is done in accordance with the Group's Non-Financial Risk policies and underlying instructions.

**Subprinciple 6.2: The Group must maintain controls to manage the Bribery and Corruption risk associated with political lobbying**

The Group must ensure that political lobbying is not used to engage in an Incident of Bribery. All Employees must adhere to the requirements set out in the Group's Stakeholder Policy when lobbying politically. In addition, all Employees must give consideration to the Bribery and Corruption risks that the potential engagement with this population could present to the Group and adhere to the requirements set out in the Group's Gifts and Hospitality Instruction.

**Subprinciple 6.3: The Group must maintain controls to manage the Financial Crime risk associated with sponsorships and donations**

The Group must ensure that payments for sponsorships and donations are not used to engage in an incident of Financial Crime.

The Group must perform due diligence on sponsorship recipients, taking into account the potential affiliation with Public Officials. The purpose and selection criteria of a sponsorship or donation must be documented and approved before any payment is made.

In addition, adequate controls must be put in place to ensure that the authorised recipient is the natural person or legal entity being paid and that there are no pending business decisions with the recipient of the sponsorship or donation payment.

**Subprinciple 6.4: The Group must maintain controls to identify, assess and manage the Financial Crime risk associated with products and services**

The Group must ensure that the product approval process set out within the Group identifies and assesses the potential exposure to Financial Crime risk of the Group, when Business Units are considering customising or altering the features and terms of a product or service for a specific or group of customer(s). This must take place prior to approving such customisation or alteration.

Before approving a new product or service, and before customising or altering the features and terms of a product or service, Business Units must ensure that Financial Crime subject matter experts are engaged for advice on the risk associated with said product and/or service.

In addition, the Group must ensure that this is done in accordance with the Group's Non-Financial Risk policies and underlying instructions.

**Subprinciple 6.5: The Group must maintain controls to identify, assess and manage the Financial Crime risk associated with geography and industry**

The Group must establish a list management framework and governance that identify, assess and manage the Financial Crime risk exposure associated with geography and industries. This includes the development of appropriate list management controls to ensure that all lists used are accurate and up-to-date.

**Subprinciple 6.6: The Group must maintain controls to detect and prevent customer impersonation attempts for Financial Crime purposes and to ensure that customers are who they say they are**

The Group must establish an authentication framework that ensures that all customer interactions have the necessary verifications in order to provide a high level of confidence that the customers with whom the Group interacts and offers products and services to are who they say they are.

The framework must take into account customer interactions throughout the end-to-end lifecycle of a customer's relationship with the Group, irrespective of the products and services offered and used. The authentication methods utilised must be regularly reviewed to ensure they at all times provide the required level of protection and customer usability.

***Principle 7: The Group must perform due diligence measures when establishing and maintaining relationships with customers and Third Parties***

The Group's due diligence framework must ensure that all customers and Third Parties are subject to due diligence measures prior to establishing a relationship and throughout the duration of the relationship. The due diligence measures must be completed prior to carrying out any transactions on behalf of the customer and before a Third Party relationship is entered into.

**Subprinciple 7.1: The Group must not establish or maintain relationships where it cannot obtain sufficient information, or mitigate the Financial Crime risks associated with the customer or associated parties**

The Group must ensure that all customers are subject to an appropriate level of due diligence at the time of on-boarding and during the duration of the customer relationship, in accordance with the customer's risk rating and the Group's other policies, instructions and procedures. Further, each customer must be assigned to a specific Business Unit which remains accountable for the ongoing oversight of that customer.

The Group must not establish a relationship with customers or associated parties where it has not obtained all relevant information as required by the due diligence requirements or maintain relationships where it has been unable to complete the due diligence processes.

Where the Group is unable to mitigate the Financial Crime risk associated with maintaining a customer relationship or where there is a suspicion of Financial Crime, adequate procedures must be in place to determine the appropriate cause of action.

Further, the Group must not maintain or enter into prohibited relationships such as relationships with shell banks. Please refer to the underlying Instructions to the Policy for further details on prohibited relationships.

**Subprinciple 7.2: The Group must develop and maintain procedures and processes for information sharing within the Group**

The Group must develop and maintain procedures and processes for sharing of information within the Group with the purpose of preventing Financial Crime.

Any sharing of information must be done in accordance with Group's Personal Data Protection Master Instruction.

**Subprinciple 7.3: The Group must perform enhanced due diligence measures where the relationship with the customer is assessed to pose an increased risk of Financial Crime**

The Group must apply enhanced due diligence measures on customer relationships that expose the Group to a higher Financial Crime risk. This requires Business Units to collect and assess additional information/documentation in relation to the customer to ensure the application of appropriate controls and to ensure that the relationship is within the Group's Financial Crime risk tolerance.

**Subprinciple 7.4: The Group must perform ongoing due diligence on all customers to ensure that customer information is accurate and up-to-date**

The Group must perform ongoing due diligence ("ODD") on all customers consisting of periodic reviews and ongoing monitoring of their activity and behaviour. This enables the Group to assess whether the customer's activities correlate with the information provided by the customer at on-boarding or when ODD was last performed, and to detect any suspicious customer activity and behaviour. Performing ODD also enables the Group to ensure that the controls and due diligence measures applied on the relationship continue to be adequate.

Minimum frequency for ODD is determined by the risk rating of the customer or where circumstances or events associated with the customer trigger an event driven ODD review.

**Subprinciple 7.5: The Group must identify and assess the Financial Crime risk associated with its customers, Third Parties and Associated Persons of the Group**

When a relationship is established or is intended to be established, the Group must ensure that the Financial Crime risk associated with the individual customer, Third Party and Associated Person of the Group is identified and assessed to determine the appropriate level of due diligence measures the customer, Third Party or Associated Person of the Group must be subject to.

**Subprinciple 7.6: The Group must identify and manage risks associated with customers and relevant parties that are considered PEPs**

The Group must develop, implement and maintain effective measures and processes to identify and mitigate the risks associated with PEPs, their known close associates and family members.

Further, the Group must maintain an appropriate definition of a PEP (including known close associates and family members) that meets the regulatory standards, as well as establish PEP specific due diligence measures and controls.

**Subprinciple 7.7: The Group must identify and manage risks associated with Public Officials**

The Group must develop, implement and maintain effective measures and processes to identify and mitigate the Bribery and Corruption risks associated with Public Officials. This includes maintaining specific due diligence measures and enhanced controls for customers, Third Parties or Associated Persons of the Group that are identified as Public Officials to address the risks identified.

The Group considers all Facilitation Payments to Public Officials in any geographic location to be an Incident of Bribery.

**Subprinciple 7.8: The Group must have controls to manage Financial Crime risks associated with correspondent relationships**

The Group must develop and maintain specific due diligence measures and controls relating to correspondent relationships, enabling an effective and consistent risk-based approach across the Group.

**Subprinciple 7.9: The Group must have controls to manage Financial Crime risks associated with countries on the EU High Risk Third Countries List**

The Group must conduct enhanced due diligence on customers carrying out transactions involving, or maintaining a registered office address in/residing in, countries on the EU High Risk Third Countries List.

**Subprinciple 7.10: The Group must develop and maintain procedures to manage relationships with Third Parties or Associated Persons of the Group that carry out aspects of the Financial Crime compliance framework on its behalf**

The Group must ensure that Third Parties and Associated Persons of the Group are subject to an appropriate level of due diligence at the time of the establishment and throughout the duration of the relationship. The due diligence must be completed before a Third Party or Associated Person of the Group carries out any aspects of the Financial Crime compliance framework on the Group's behalf.

In addition, the Group must develop and implement appropriate standards and procedures when relying on, or outsourcing Financial Crime risk management activities to Third Parties or Associated Persons of the Group. Further, whilst Financial Crime compliance responsibilities can be performed by Third Parties or Associated Persons of the Group, the Group remains ultimately accountable for their activities.

***Principle 8: The Group must conduct risk-based monitoring and screening to identify Financial Crime risk***

The Group must develop and implement transaction monitoring and screening controls to identify its Financial Crime risk exposure, potential suspicious or inconsistent activity, PEP relationships and potential adverse media.

**Subprinciple 8.1: The Group must conduct risk-based transaction monitoring to identify Financial Crime**

The Group must monitor all customer relationships on an ongoing basis and review customer transactions to identify complex and/or unusual transactions, as well as unusual patterns of transactions and activities that have no apparent economic or legitimate purpose. Due to the significant volume of transactions processed, the Group must develop risk-based scenarios, typologies, rules and thresholds to identify such activity.

**Subprinciple 8.2: The Group must apply risk-based Sanctions screening against relevant Sanctions lists**

The Group must screen all relevant information related to customers, potential customers, relevant associated parties, transactions and business activities against relevant Sanctions lists to ensure compliance with Sanctions.

The Group must ensure that the screening controls are applied prospectively prior to engaging in a relationship or a transaction and that any potential Sanctions-related alerts and concerns identified through application of those controls are resolved prior to completing the engagement or transaction.

**Subprinciple 8.3: The Group must conduct screening to identify which customers and relevant parties should be classified as PEPs**

The Group must ensure that all customers and relevant parties are screened against PEPs lists to determine whether there are any PEPs, or known close associates and family members of PEPs within the Group. If hits are identified, these should be investigated to determine whether they are genuine and if so, appropriate due diligence should be applied.

**Subprinciple 8.4: The Group must conduct risk-based searches to help identify potential adverse media associated with its customers, Third Parties and where relevant Associated Persons of the Group**

The Group must apply risk-based media searches to help identify whether any customers, relevant associated parties, Third Parties and where relevant Associated Persons of the Group are subjects of Financial Crime related adverse media. Relevant hits should be investigated to determine whether they are true and if so, their materiality in respect of the relationship with the Group should be assessed.

**Subprinciple 8.5: The Group must maintain a list management framework to ensure up-to-date and accurate screening for Sanctions and PEPs**

The Group must establish a list management framework and governance that defines the relevant internal and/or external Sanctions and PEP lists to be applied in screening. This includes the development of appropriate list management processes to ensure that all lists used for screening are accurate and up-to-date.

**Subprinciple 8.6: The Group must conduct risk-based ongoing monitoring and oversight of all relationships with Third Parties and Associated Persons of the Group (where relevant) to identify Financial Crime risks**

The Group must implement and maintain effective controls and processes to ensure all relationships with Third Parties and where relevant, Associated Persons of the Group are subject to ongoing monitoring and oversight of their performance and compliance with the requirements of the agreement to identify Financial Crime risk.

***Principle 9: The Group must ensure that suspicious activity, incidents of Financial Crime or potential Financial Crime violations are investigated and reported to the competent authorities***

The Group must ensure that it implements and maintains effective controls and processes to ensure that suspicious activity, incidents of Financial Crime or potential Financial Crime violations are reported to the competent authorities in a timely manner.

**Subprinciple 9.1: The Group must investigate and report knowledge or information of transactions, assets or activities that are deemed to be suspicious**

The Group must ensure that if there is any concern relating to transactions, assets or activity that may be connected to money laundering, terrorist financing or any other type of Financial Crime, this must be investigated and reported to the Suspicious Activity Reporting Office ("SARO") or local Money Laundering Reporting Officer ("MLRO") as an Unusual Activity Report ("UAR"). The investigation process must include controls to prevent the customer being tipped off.

Where the unusual activity is determined to be suspicious, the relevant SARO or local MLRO must report the activity to the local Financial Intelligence Unit ("FIU") or equivalent competent authority.

**Subprinciple 9.2: The Group must investigate potential Sanctions violations to determine appropriate action, and when necessary, report those to the relevant authorities**

The Group must ensure that potential Sanctions violations or material Sanctions concerns are reviewed by Group Compliance in order to determine whether it requires further action. Any action taken will depend on the applicable Sanctions implicated by the concerns. These may include, among others, freezing of funds, rejecting a transaction or declining a relationship and reporting to the competent authorities.

Where a transaction, relationship or other activity is determined to be subject to applicable Sanctions, Group Compliance must report it to the competent authorities.

**Subprinciple 9.3: The Group must investigate incidents of Fraud (internal and external) or potential Fraud (internal and external) violations to determine appropriate action, and when necessary, report those to the relevant authorities**

The Group must ensure that incidents of Fraud (internal and external) or potential Fraud (internal and external) violations are reviewed and escalated in accordance with the Group's policies and underlying instructions in order to determine whether it requires further action. Where deemed necessary, reporting must be done to the competent authorities in a timely manner.

***Principle 10: The Group must ensure that its Employees have adequate competence and awareness about Financial Crime compliance requirements and controls by providing regular training and communication***

The Group must provide Employees, with training on the regulatory requirements the Group must adhere to and Financial Crime risk to which the Group is exposed. This includes specific, tailored training for Employees that fulfil roles with higher Financial Crime risk exposure.

Training is an integral part of the Group's Financial Crime risk management. Completion of training must be documented and monitored through appropriate MI metrics, and non-completion of training must be taken seriously through appropriate consequence management.

***Principle 11: The Group must ensure that records relevant for Financial Crime compliance are retained to ensure auditability and investigation***

The Group must retain accurate electronic records concerning customer, and Third Party information, risk assessments, transactions, reviewing and investigation of alerts and other relevant information, including material decisions, approvals and documentation related to the management of Financial Crime risk.

Employees must not engage in fraudulent record keeping activities, including but not limited to theft, Fraud, forgery and fabrication of false evidence records, defacement or destruction of any record belonging to the Group, the Group's customers, Employees or other Associated Persons of the Group when acting on behalf of the Group.

All records must comply with relevant data retention, data privacy and data protection laws and regulations. At a minimum, all records should be kept for a period of five years from the date the customer relationship ended or a one-off transaction was processed.

***Principle 12: The Group must assess and monitor the effectiveness of its Financial Crime compliance framework through regular assurance and control testing including audits***

The Group must regularly conduct risk-based assurance and control testing of its Financial Crime compliance framework. The methodologies and frequency of testing should be appropriate to the level and sophistication of the risks.

The Group must ensure that the functions performing assurance and control activities have sufficient skills, expertise, resources and authority within the organisation to effectively identify weaknesses and deficiencies, inform enhancement opportunities as well as inform the Financial Crime risk profile for the purposes of management reporting.

***Principle 13: The Group must ensure that all Financial Crime compliance controls and processes are adequately managed through business continuity management arrangements***

Financial Crime controls and processes are interlinked with the ability to process transactions, deliver products and services, and on-board and maintain customers and other relationships. Any disruption in controls and processes may have a significant impact on the Group's compliance with its Financial Crime obligations, but may also result in significant business and market disruptions.

As it is critical to ensure compliance while also ensuring that the Group continues to provide and deliver services, the Group must ensure that all critical Financial Crime related controls and processes have appropriate business continuity management arrangements and protocols implemented to ensure compliance and avoid business disruptions.

***Principle 14: The Group must engage, cooperate and communicate with supervisors, competent authorities and law enforcement agencies***

The Group must ensure that any interaction or engagement with supervisors, competent authorities and law enforcement agencies is carried out in accordance with the Group's policies and underlying instructions.

Group Compliance must be immediately informed of any Financial Crime related request received from supervisors, competent authorities or law enforcement agencies. Group Compliance must ensure that all information requests are promptly responded to and managed in accordance with relevant data protection and bank secrecy requirements, as necessary.

## **5. Escalation**

The Group's Escalation Policy sets the requirements for appropriate and timely internal reporting of potentially problematic cases across the Group. The requirements in the Group's Escalation Policy must always be considered in relation to violation of the Group's obligation to prevent and mitigate Financial Crime risk, with adherence to other related policies and governing documents.

Please refer to the Group's Escalation Policy and underlying instructions.

## **6. Review**

The administrator must review and update the Policy at least annually or more frequently if required. Events which may cause a need for a review by the administrator include changes to relevant applicable regulation and legislation.