CTFG_Policy_015 English Version

CHOW TAI FOOK JEWELLERY GROUP

周 大 福 珠 寶 集 團

Chow Tai Fook Jewellery Group Limited

<Group Anti-Money Laundering Policy>

April 2020

INTRODUCTION, OBJECTIVE AND POLICY STATEMENT

1. Chow Tai Fook Jewellery Group Limited and its subsidiaries (the "Group") acknowledges an importance of preventing money laundering ("ML"), terrorist financing ("TF"), proliferation financing, tax evasion, and sanction violation. To safeguard the Group against the risk of becoming involved in ML, TF, proliferation financing, tax evasion and sanction violation, and the reputation risks associated with money laundering, the Group has established this Group Anti-Money Laundering ("AML") Policy to ensure timely risk identification and establishment of appropriate controls to mitigate the above risks.

2. The Group is committed to prohibiting and combating ML, TF, sanctions violations and other criminal activities by complying with relevant AML laws and regulations in jurisdictions where it operates.

GOVERNANCE AND OVERSIGHT

3. A comprehensive assessment of ML/TF and sanctions compliance risks should be performed by relevant business units from time to time and in any case prior to any circumstances that could change the risk profile of the Group. The assessment should be performed in accordance with the Group's Risk Management and Internal Control Governance Framework and practices.

4. AML, Counter-Financing of Terrorism ("CFT") and sanctions will be discussed in the Group Risk Management Committee ("GRMC") meetings on an as-needed basis to ensure that appropriate information regarding ML, TF and sanctions risks is communicated to senior management in a timely manner so that they are equipped with adequate information to make informed decisions to manage these risks.

INTERNAL CONTROLS

Know your customers/counterparties and customer due diligence ("CDD")

5. Performing CDD enables the Group to understand the customers and counterparties and put in place appropriate measures to prevent that the Group is misused for ML and TF. The Group adopts a risk-based approach to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

6. In respect of customers, CDD must be performed when (i) the transactions appear suspicious; or (ii) the customer requests to make a large cash transaction.

7. In respect of counterparties, CDD must be performed when (i) the transactions appear suspicious; (ii) the counterparty is incorporated or operated in high risk countries, for example countries identified by the Financial Action Task Force ("FATF") as having deficient systems to prevent ML and TF; or (iii) the counterparty sources raw materials/finished products from high risk countries.

8. Frontline units or back office business units should apply enhanced due diligence ("EDD") measures in relation to a business relationship or transaction that presents a high ML/TF risk, which means taking additional measures to identify and verify the customers' and counterparties' identity and source of funds and applying additional ongoing monitoring.

9. After the establishment of a business relationship, ongoing monitoring must be performed on the counterparties' profiles to understand the counterparties' activities, update the knowledge of the counterparties and detect potentially unusual or suspicious activities. High risk counterparties are subject to at least an annual review. Medium risk counterparties are subject to a review every two years. Review should also be performed when there is a change in beneficial owners and/or persons of control of the counterparties.

Money Laundering Reporting Officer ("MLRO")

10. The Group appoints MLROs to supervise all aspects of the Group's AML/CFT. MLROs play an active role in the identification and reporting of suspicious transactions.

11. Principal functions of MLROs include (i) reviewing internal suspicious reports and, in light of all available relevant information, determining whether it is necessary to make a report to senior management and relevant regulatory bodies or law enforcement agencies; and (ii) maintaining a record management system for appropriate storage and retrieval of documents and records.

Suspicious transactions reporting

12. The Group diligently monitors transaction for suspicious activities. The Group has the obligation to report any suspicion or knowledge of money laundering with regulatory bodies or law enforcement agencies.

13. In respect of internal reporting, the Group has developed an internal reporting process to ensure proper and timely reporting of suspicious activities. When there is a suspicion or knowledge of ML/TF, frontline units or back office business units should file an internal Suspicious Transaction Report ("STR") to respective regional AML Task Force and senior management through the internal reporting process.

14. In respect of external reporting, the Group appoints MLROs as central reference point for reporting suspicious transactions and also as the main point of contact with regulatory bodies or law enforcement agencies**.** It is the discretion of the MLROs to determine whether or not it is necessary to make a report to the relevant regulatory bodies or law enforcement agencies after receiving the internal STRs from regional AML Task Force.

Transaction review

15. Periodic review of transactions enables the Group to identify or detect any anomalies in the transactions, potential suspicious activities, trends or patterns. Transaction reviews in respect of customers and counterparties will be carried out on an annual basis. The assessment/analysis performed on the transaction review will be documented in writing and provided to senior management for review.

Staff training and awareness building

16. Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. The Group will provide ongoing training to all staff of the Group in order to establish and maintain their vigilance in AML and CFT matters. Apart from the general training, the Group also provides regular refresher training to MLROs and regional AML Task Force to keep them abreast of AML and CFT requirements or developments.

17. The content and frequency of the training is tailored to the specific risks faced by the operation units and pitched according to the job functions, responsibilities and experience of the staff.

Record keeping

18. The Group recognizes the importance of record keeping to AML investigation which allows for swift reconstruction of individual transactions and provides evidence for prosecution of criminal activities including ML. Our regional AML Task Force is responsible for ensuring the AML records (for example, records of CDD checks, records of transactions and details of action taken in respect of internal and external STR) are maintained properly.

19. We keep our records in the form of original documents or copies in either hard copy or electronic form. All electronic records are subject to regular and routine backup.

20. We keep the records at a minimum for (i) five years after the end of the business relationship; or (ii) five years after the date of a transaction was completed.

Sanctions compliance

21. The Group is committed to identifying, mitigating and managing the risk of sanction violations and complying with the relevant economic and trade sanctions laws in all jurisdictions in which it operates.

22. At the establishment of the relationship with customers, counterparties or staff, screening must be performed in respect of specific customers, counterparties (including their beneficial owners, persons of control and connected parties) and staff against a database of names and particulars of terrorists and parties designated by the United Nations Security Council or its committees and the Office of Foreign Assets Control of the Department of Treasury of the United States of America ("Sanctions Database") to ensure they are not terrorists or designated parties.

23. After the establishment of the relationship, screening must be performed in respect of specific customers, counterparties (including their beneficial owners, persons of control and connected parties) and staff against all new and any updated designations to the Sanctions Database on an ongoing basis.

24. If the customer, counterparty or staff is confirmed to be a terrorist or a designated party, the business or employment relationship should be terminated and an external STR should be filed to the regulatory bodies or law enforcement agencies as soon as possible.