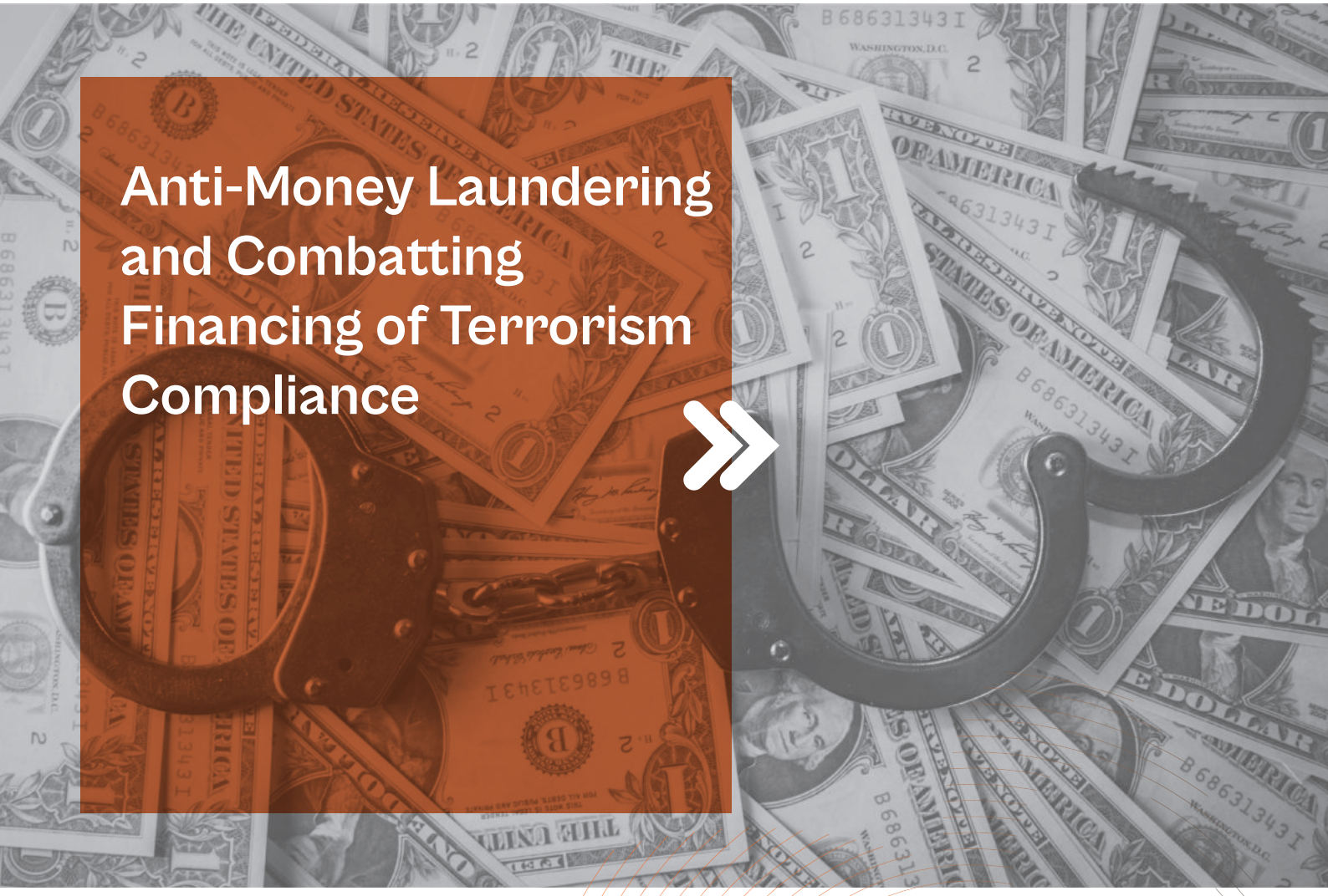
CHRYSCAPITAL



Anti-Money Laundering and Combatting Financing of Terrorism Compliance

Release date	10 November 2020
Prepared by	Puneet Chadha
Distribution	All Employees and Partners
Reviewed by	Ashley Menezes

Amendment Sheet			
Sr. No.	Date	Revision Status	Reason for Amendment
1.	10 November 2020	Initial Release	NA
2.	3 April 2023	Amendment	Renewed policy

I. Purpose of the AML-CFT Policy:

This document aims to lay out the objectives, scope, and philosophy of ChrysCapital's Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) AML-CFT Policy (the "AML-CFT Policy").

ChrysCapital seeks to maintain the integrity and reputation of its business and to ensure compliance with the Prevention of Money Laundering Act, 2002 (PMLA) and CFT regulations.

ChrysCapital recognizes the importance of detecting and preventing the laundering of money and financing of terrorism through the financial system. This AML-CFT Policy is a set of guidelines and procedures that ChrysCapital will implement to comply with the legal and regulatory requirements of the PMLA and CFT regulations in India so as to help ChrysCapital in protecting itself from potential legal and financial consequences associated with non-compliance.

II. Objective of the AML-CFT Policy:

The main objectives of this AML-CFT Policy are:

1. To prevent ChrysCapital from being used as a vehicle for money laundering or terrorism financing activities.
2. To comply with the legal and regulatory requirements of the PMLA regulations.
3. To identify and mitigate the risks associated with money laundering and terrorism financing.

III. Definitions:

For the purposes of this AML-CFT Policy, the following terms are defined as follows:

1. Anti-Money Laundering (AML): refers to the set of measures, processes, and procedures aimed at preventing, detecting, and reporting money laundering activities.
2. Customer Due Diligence (CDD): refers to the process of verifying the identity of a customer and assessing the risk associated with that customer.
3. Countering the Financing of Terrorism (CFT): refers to the measures, processes, and procedures aimed at preventing, detecting, and reporting the financing of terrorism.
4. Enhanced Due Diligence (EDD): refers to a higher level of due diligence that is conducted in high-risk situations.
5. Money Laundering (ML): refers to the process of disguising the proceeds of illegal activities as legitimate funds.
6. Politically Exposed Person (PEP): refers to an individual who is or has been entrusted with a prominent public function, such as a head of state, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official.

IV. Scope and application of the AML-CFT Policy:

The scope of this AML-CFT Policy applies to all operations, activities, and transactions conducted by ChrysCapital. The AML-CFT Policy covers all employees, agents, and representatives of ChrysCapital, as well as any third-party service providers that may be engaged to perform services on behalf of ChrysCapital.

The AML-CFT Policy is intended to be comprehensive and covers all aspects of ChrysCapital's operations that may be vulnerable to money laundering or the financing of terrorism. The AML-CFT Policy sets out the processes, procedures, and controls that ChrysCapital will implement to identify, assess, and mitigate the risk of money laundering and terrorism financing.

The AML-CFT Policy applies to all types of transactions, including but not limited to, the opening of accounts, the execution of transactions, and the ongoing monitoring of customer relationships. The AML-CFT Policy also applies to the development and implementation of systems and controls to detect and prevent money laundering and terrorism financing.

The AML-CFT Policy will be reviewed and updated on a regular basis to ensure that it remains relevant and effective in addressing the evolving threat of money laundering and terrorism financing. ChrysCapital will also conduct regular risk assessments to identify any new or emerging risks and will take appropriate action to mitigate these risks.

V. Risk Management Process and Procedures:

Have an effective risk management system in place to ensure compliance with the Prevention of Money Laundering Act (PMLA) and the Countering the Financing of Terrorism (CFT) regulations is an important

step towards ensuring financial compliance. The following is a detailed explanation of the risk management process and procedures to be followed by ChrysCapital:

1. Risk Assessment: The first step in the risk management process is to assess the risk of money laundering and terrorism financing. ChrysCapital will determine the risk of money laundering and terrorism financing based on the nature of its business, the types of customers that it serves, and the geographical locations that it operates in. ChrysCapital will also assess the risk of money laundering and terrorism financing based on the results of its customer due diligence process.
2. Customer Due Diligence: ChrysCapital will have a robust customer due diligence process in place to assess the risk of its customers. The customer due diligence process will include obtaining and verifying the identity of its customers, assessing the source of its customers' funds, and monitoring its customers' transactions for suspicious activity.
3. Ongoing Monitoring: ChrysCapital will have a system in place to monitor its customers' transactions on an ongoing basis. ChrysCapital will monitor its customers' transactions for transactions that are inconsistent with the customer's normal behaviour or are indicative of money laundering or terrorism financing. ChrysCapital will also monitor its customers' transactions for transactions that are structured to avoid reporting requirements or that are structured in a manner that is indicative of money laundering or terrorism financing.
4. Reporting Suspicious Transactions: ChrysCapital will have a process in place to report suspicious transactions to the Financial Intelligence Unit (FIU). ChrysCapital will file a Suspicious Activity Report (SAR) within 7 days of the date that it becomes aware of the suspicious transaction. The SAR will include information about the customer, the transaction, and the reason for filing the SAR.
5. Record Keeping: ChrysCapital will keep records of all SARs that it files and all supporting documentation for a period of 10 years. ChrysCapital will also keep records of all customer due diligence information and all ongoing monitoring information for a period of 10 years.
6. Training and Awareness: ChrysCapital will provide regular training and awareness programs for its employees on the risks of money laundering and terrorism financing and the steps that they should take to mitigate these risks. The training will include a discussion of the ChrysCapital's risk management AML-CFT Policy and procedures, the red flags of money laundering and terrorism financing, and the steps that the employees must take if they suspect that a transaction is suspicious.

VI. Types of Customers:

For the purposes of the Anti-Money Laundering and Countering the Financing of Terrorism (AML-CFT) AML-CFT Policy, a customer is defined as any individual or entity that engages in transactions with ChrysCapital, whether on a one-time or ongoing basis. This includes, but is not limited to, the following:

1. Institutional investors: This includes pension funds, endowments, foundations, and insurance companies that invest in private equity funds.
2. High net worth individuals: These are individuals with significant wealth who invest in private equity funds.
3. Family offices: These are investment entities established to manage the wealth of wealthy families.

4. Corporate clients: This includes corporations and other entities that invest in private equity funds.
5. Service providers: This includes accountants, lawyers, and other professionals that provide services to ChrysCapital and their investors.

This definition is intended to be inclusive and covers all types of customers that ChrysCapital may deal with, regardless of the size or nature of their transactions. The definition is also intended to capture all types of relationships that ChrysCapital may have with its customers, including but not limited to, the opening of accounts, the execution of transactions, and the ongoing monitoring of customer relationships.

VII. Categorization of Customers as per the Risk Level:

ChrysCapital will categorize its customers based on their level of risk for the purposes of Anti-Money Laundering and Countering the Financing of Terrorism (AML-CFT) compliance. The following is a detailed explanation of the categorization of low, medium, and high-risk customers:

1. Low-Risk Customers: Low-risk customers are those that pose a low risk of money laundering or terrorism financing. They may include customers with a low net worth or low transaction volumes, customers with a long-standing relationship, or customers who operate in low-risk jurisdictions. Low-risk customers typically require minimal due diligence and ongoing monitoring.
2. Medium-Risk Customers: Medium-risk customers are those that pose a moderate risk of money laundering or terrorism financing. They may include customers with a higher net worth or higher transaction volumes, customers who operate in high-risk jurisdictions, or customers who have a higher risk of corruption or fraud. Medium-risk customers typically require more extensive due diligence and ongoing monitoring.
3. High-Risk Customers: High-risk customers are those that pose a high risk of money laundering or terrorism financing. They may include customers who operate in high-risk jurisdictions, customers who have a high risk of corruption or fraud, or customers who have a high net worth or high transaction volumes. High-risk customers typically require the most extensive due diligence and ongoing monitoring.

It is important to note that the categorization of customers as low, medium, or high-risk is not a static process and may change over time as the customer's risk profile evolves. ChrysCapital will continuously assess and reassess the risk posed by each customer and update the categorization accordingly.

VIII. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD):

Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) are critical components of ChrysCapital's AML-CFT compliance program. The purpose of CDD and EDD is to assess the customer's risk profile and ensure that ChrysCapital is not engaging in business with individuals or entities that pose a high risk of money laundering or terrorism financing. The following is a detailed explanation of the CDD and EDD process of customers of ChrysCapital as per Indian PMLA and CFT regulations:

1. Customer Identification: The first step in the CDD and EDD process is to identify the customer.

ChrysCapital will obtain and verify the customer's name, address, and identity, as well as the beneficial owners of the customer. ChrysCapital will also obtain and verify the customer's source of funds and source of wealth.

2. Risk Assessment: The next step is to assess the customer's risk profile. ChrysCapital will determine the customer's risk category based on the customer's country of origin, the nature of the customer's business, the customer's source of funds, and the customer's past behaviour. ChrysCapital will also assess the customer's exposure to money laundering or terrorism financing.
3. Customer Due Diligence (CDD): ChrysCapital will conduct customer due diligence (CDD) on the customer. CDD is a process of gathering information about the customer to determine the customer's risk profile. ChrysCapital will obtain and verify the customer's identification and contact information, as well as the customer's source of funds and source of wealth. ChrysCapital will also obtain and verify information about the customer's business, including the ownership and structure of the business, the business activities, and the customer's reputation and history.
4. Enhanced Due Diligence (EDD): In some cases, ChrysCapital will be required to conduct enhanced due diligence (EDD) on the customer. EDD is a more in-depth process of gathering information about the customer and is typically required for high-risk customers. ChrysCapital will obtain and verify information about the customer's political exposure, the customer's reputation and history, and the customer's source of funds and source of wealth. ChrysCapital will also be required to obtain additional information about the customer's business activities, such as the customer's business relationships and the customer's suppliers and customers.
5. Ongoing Monitoring: ChrysCapital will also conduct ongoing monitoring of the customer's transactions to ensure that the customer's risk profile remains low and to detect any suspicious activity. ChrysCapital will also periodically review the customer's risk profile and update the due diligence information as necessary.

IX. Monitoring and Reporting of Suspicious Transactions:

1. Risk Assessment: The first step in the process of monitoring and reporting suspicious transactions is to conduct a risk assessment. ChrysCapital will assess the risk of money laundering and terrorism financing associated with its customers, products, services, and geographic locations. Based on the risk assessment, ChrysCapital will develop and implement an AML-CFT program that is commensurate with the level of risk.
2. Transaction Monitoring: ChrysCapital will also monitor its customers' transactions for suspicious activity, such as transactions that are inconsistent with the customer's profile or transactions that are unusual for the type of customer or the type of business. ChrysCapital will also review transactions that are flagged by the transaction monitoring software.
3. Suspicious Activity Reporting (SAR): If ChrysCapital detects suspicious activity, it will report the suspicious activity to the relevant authorities. In India, ChrysCapital will report the suspicious activity to the Financial Intelligence Unit (FIU-IND). The report will be made within seven working days of the detection of the suspicious activity. The report will include a detailed description of the suspicious activity, including the identity of the customer, the transaction involved, and the reason for the suspicion.

Examples of Suspicious Transactions:

1. Large or frequent cash deposits or withdrawals.
2. Transactions that are inconsistent with the customer's profile or business activities.
3. Transactions that are structured to avoid reporting requirements.
4. Transactions that are inconsistent with the customer's normal behaviour or pattern of transactions.
5. Transactions that are associated with a high-risk country or a high-risk customer.
6. Transactions that involve individuals or entities that are subject to sanctions or that have a history of money laundering or terrorism financing.

X. Reporting to Financial Intelligence Unit:

The Compliance Officer will report information relating to suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director,

Financial Intelligence Unit, India,

6th Floor, Hotel Samrat, Chanakyapuri,

New Delhi - 110021

ChrysCapital Advisors LLP

502 Ceejay House, Dr. Annie Besant Road,
Worli, Mumbai 400 018. INDIA.

+91 22 4066 8000

www.chryscapital.com