ChangeNOW

RULES
of Anti-Money Laundering and Combating The Financing Terrorism
Compliance Control

1. Definitions

1.1. What is Anti-Money Laundering and Combating the Financing Terrorism compliance control?

Set of measures for detection and prevention money laundering and terrorists financing.

1.2. What is money laundering?

1.2.1. Conversation or transfer of property derived from criminal activity, or, property obtained instead of such property, knowing that such property is derived from criminal activity, or, from an act of participation in such activity, for the purpose of concealing, or disguising the illicit origin of the property, or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions.

1.2.2. The acquisition, possession or use of property derived from criminal activity, or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein.

1.2.3. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained
instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

1.3. What is terrorist financing?

The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organisations or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

1.4. What is a high-risk country?

A country specified in a delegated act adopted on the basis of Anti-Money Laundering Act (2006).

1.5. What is the MLTFPA?

The legal act that regulates the activities of credit and financial institutions, other undertakings and institutions specified in the Anti-Money Laundering Act (2006) which involve the prevention of money laundering and terrorist financing.

In Seychelles: Anti-Money Laundering Act (2006).

1.6. What is a company?

CHN Group Limited, a company incorporated and existing under the laws of Seychelles under IBC NO 219011 and having registered office at House of Francis, Room 303, Ile Du Port, Mahe, Seychelles.

Postal Address: Newtonlaan 115, Utrecht, 3584 BH, Netherlands

1.7. Who is a customer?
A person or a legal entity who uses, or has used, services offered by company.

1.8. What is a transaction monitoring?
Every single investigation conducted by a company about a customer, KYC and other measures.

1.9. Who is an ultimate beneficial owner of a legal entity (UBO)?
Ultimate beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal entity or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owner or a beneficiary under a life or other investment linked insurance policy. An UBO is a private individual owning or controlling more than 25% of a legal entity.

1.10. What is the Financial Intelligence Unit?
Seychelles Financial Intelligence Unit (FIU).

2. Standard Procedure for Customer Identification and Verification

2.1. The company has automatic risk-management system that helps the company to identify suspicious transactions.
The company has right to identify its customers who wants to use the company's services on the basis of an identity (especially if the transaction seems to be suspicious).

2.2. If the customer is a private individual, the company has the right to ask he or she to provide:
2.2.1. full name;
2.2.2. personal identification code or, if none, the date of birth and the place of residence;
2.2.3. if the customer is in fact representing another private individual being the real customer (under a power of attorney, or in the case of inheritance, or any other way) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer;
2.2.4. whether the customer is a politically exposed person (PEP), a family member of a PEP or a person known to be a close associate with a PEP.

2.3. The company may ask the following valid documents serve as basis for identification:
2.3.1. an identity card;
2.3.2. a passport;
2.3.3. a diplomatic passport;
2.3.4. a driving license if the document shows the name, photo or face image, signature or signature image and date of birth or personal identification code of its holder.

2.4. If the customer is a legal entity, the company has the right to ask it to provide:

2.4.1. legal name;
2.4.2. date of incorporation;
2.4.3. place of incorporation and registered address
2.4.3. description of nature of the customer's business.

2.5. The documents mentioned in the section 2.10. may serve as basis for the identification of the legal entity.

2.6. In identifying a person, company may check the validity of the identity document, make sure
the person matches the information on the document and check the age of the person. If in doubt about the identity of the person, company may request additional information about the person or request for the additional actions (such as making selfie or screen of the wallet, or making test transaction). Upon sending a document that does not match the person or is invalid, company must refuse the customers' transaction. If the customer refuses provide the documents upon the company's request, the company has right to refuse the customers' transaction.

2.7. The company has the right to verify the correctness of the customer data, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified in the section 2.3. or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document, or can be identified using means of electronic identification and trust services for electronic transactions, no additonal details on the document need to be retained.

2.8. The company has the right to identify the beneficial owners (UBOs) and, for the purpose of verifying their identities, taking measures to the extent that allows the company to make certain that he/she knows who the beneficial owners are, and understands the ownership and control structure of the customer, or of the person participating in the transaction.

2.9. The company verifies the correctness of the information of a legal entity, using the information originating from a credible and independent source for that purpose. When company is able to verify the information through such direct access, the submission of the documents specified in section 2.10. does not need to be demanded from the customer.

2.10. If the customer is a legal entity (for example a company), the company has the right to ask it to provide in addition to the information in sections 2.4. and 2.8., a Commercial Registry (or Company House or similar, depending of the country of origin) extract for the legal entity authenticated by a public notary and/or legalized and/or certified with an apostille, unless otherwise provided for in an international agreement also showing the rights of representation for that legal entity.

2.11. A representative of a legal person must, at the request of company, for example when the right of representation does not appear in the submitted documents, submit a document certifying his or her powers (a power of attorney), which has been authenticated by a public notary and/or legalized and/or certified with an apostille, unless otherwise provided for in an international agreement.

2.12. The company may ask additional information about the customer in case of any suspicion about the customer's identity information or the customer's behavior. Such additional information asked should be relevant to the raised risks which, when obtained, may prove that the risks are in fact explainable.

2.13. The company can also collect information about customers email address, phone number and date of birth and add this to the customer KYC file.

2.14. The company may cross-check the customer through the internal and external databases of device fingerprints, address, name, e-mail, ID code and all other data that is available in order to detect double registrations or multiple accounts of the customer.

2.15 The company may cross-check the customer through appropriate sanctions lists including but not limited to:

- OFAC SDN
- United Nations Security Council Sanctions List
- World Bank - Ineligible Firms And Individuals List
- EU - Financial Sanctions List
- UK - HMT Financial Sanctions List
- AU - DFAT Consolidated Sanction List
- US - Bureau Of Industry And Security List
- CH - SECO Sanction List
- US - Department Of State Nonproliferation Sanctions List
- Interpol Wanted List

3. Enhanced Due Diligence Procedure

3.1. The company can undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such as:
3.1.1. there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
3.1.2. the customer is a politically exposed person (except for a local politically exposed person, their family members or a close associates);
3.1.3. the customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;
3.1.4. the customer is from a risk country, or from a territory that is considered a low tax rate territory.

3.2. Other factors that are referring to a higher risk pertaining to the customer:
3.2.1. when there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose;
3.2.2. customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
3.2.3. the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;

3.2.4. the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

3.3. Other factors that are referring to a higher risk pertaining to the product, service, transaction or delivery channel:
3.3.1. products/services that favors anonymity;
3.3.2. payments received from unknown or unassociated third parties.

3.4. The company can identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks. Depending on the case, company may apply one or several of the following due diligence measures:
3.4.1. verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
3.4.2. gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
3.4.3. gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the extensibility of the transactions.

4. Collecting Data and Record-Keeping

4.1. The company has the right to keep all records about our customer and our customers' behaviour in such a way that it can always be presented to inspectors checking the recorded transactions.

4.2. The company is responsible for keeping all relevant data.

4.3. The personal data of a customer, a customer's transaction and other relevant information can be stored for no less than 7 year after termination of the business relationship.

4.4. If a customer fails to submit all necessary documents and relevant information, or, if on the basis of the documents provided company has a suspicion that money laundering or terrorist financing might be involved, company has right not to make a transaction with that customer and shall record as many customer details as possible that will later help to identify the customer.

5. Risk Based Approach

5.1. The company analyzing the customer and his/her behaviour may undertake investigative efforts that are proportional to the risk and complexity of the case and collect evidence using observations gathered in the case.

5.2. If the company identifies any additional risks, they will need to conduct investigative research to understand these risks in the context of the case.

5.3. Additional evidence will be needed to support the review and understanding if additional risks are identified.

5.4. The following questions may help to determine whether a transaction is suspicious or whether there is a risk of money laundering or terrorist financing:
5.4.1. is it inconsistent with the customer's known activities?
5.4.2. is the size of the transaction inconsistent with the normal activities of the customer as determined at the initial identification stage?
5.4.3. are there any other transactions linked to the transaction in question of which our company is aware of and which could be designed to disguise money and divert it into other forms of other destinations or beneficiaries?

6. Interaction with the Customer

6.1. The company may always contact the customer to clarify the information given or ask for additional information which is needed for the customer identification, or to address the risks of the case.

6.2. The company may refuse to provide a service to the customers without asking additional information from the customer.

7. Monitoring the Transactions

7.1. A transaction monitoring case may be initiated based on a behaviour trigger of the customer or manually by company. A company has the right to investigate every initiated case.

7.2. The company should determine what the risks of the case are. Each risk should be addressed and documented.

7.3. The company has right to conduct a pre-research and check whether the customer was checked previously and what were the concerns earlier.

7.4. The company has right to conduct customer research to determine the customer's profile and identify the source and origin of the funds used in a transaction.

7.5. The company can conduct an activity research of the customer and determine whether it is in line of the customer profile or if the behaviour seems suspicious. Activity research may include all observations about the customer's behaviour and any red flags in the activity.

7.6. The company has the right conduct research on all the counterparties if it is applicable in the case.

7.7. The case review may vary on the evidence needed to collect about the customer and his/her activity. Company should use a risk-based approach to address the risks proportionally.

7.8. The company must document all the findings about the customer and customer's behaviour which support the decision of company about closing.

8. Understanding the Customer, the Customer's Activity

8.1. During the transaction monitoring case review, company can collect enough evidence to mitigate the risks alerted. For this reason, company has right to research and use the following information:
8.1.1. the customer's age;
8.1.2. location of the customer;
8.1.3. the history of the customer's transactions;
8.1.4. the type of transactions;
8.1.5. any negative information associated with the customer;
8.1.6. any factors that cause the customer to be considered a high risk;
8.1.7. other information which helps to understand the customer, the customer's activity and its counter parties.

9. Decision-Making

9.1. After each case review, company will make a final decision about whether to refuse to provide a service to the customer or close the case, based on the evidence collected for the case, and provide a final conclusion that supports the decision made.

9.2. While making a final decision, the company has the right:
9.2.1. finish the research about the customer, the customer's behaviour and the customer's counter parties;
9.2.2. understand the evidence collected and look for indications of unusual activities;
9.2.3. consider each piece of evidence on its own and consider all evidence at the same time;
9.2.4. if two pieces of evidence contradict each other, look at them together;
9.2.5. identify which pieces of evidence have the greatest impact on the analysis;
9.2.6. identify each piece of evidence that has at least impact on your analysis;
9.2.7. determine which theory is most strongly supported by the evidence.

10. Reporting Procedure of Suspicious and Unusual Transactions

10.1. If the company has a suspicion that it may be dealing with a suspicious or unusual transaction, the company may also receive the reason for reporting and identification information about the customer.

10.2. The company is not on duty to notify the customer is suspected.

10.3. The company may consider each report to determine whether it gives rise to grounds for suspicion. Where such suspicion is determined, a suspicious transaction report made the company may be sent to the Financial Intelligence Unit.

10.4. In case of suspicion of terrorist financing, company can identify the risk customer if the risks belonging to a customer cannot be reasonable mitigated or explained.

10.5. The risks of terrorist financing include, but are not limited to:
10.5.1. the individual was born in a high-risk country;
10.5.2. the individual is a citizen of a high-risk country;
10.5.3. the individual has a place of residence in a risk country or the legal entity is incorporated in a high-risk country;
10.5.4. the natural person is associated with a legal person or another entity registered in a high-risk country.

11. Violation of Duty to Register Information and Keep Records

Any violation of the duty to register information and to keep records as prescribed by the Anti-Money Laundering Act (2006) shall be disciplined in accordance with the law.

12. Requests From the Financial Intelligence Unit

Upon the request of a supervision officer of the Financial Intelligence Unit all necessary documents and information may be provided by the company to the inspectors, and the customers agree with this.

13. Persons responsible for ensuring AML compliance:

ChangeNOW AML Compliance Officer:

DocuSigned by:
Luan Kleber Gomes Farias
1CDBF06DBEA74E6...