WBB CONSULTANCY SA reg #18874 IBC 2010
Cedar Hill Crest, Villa, Kingstown,
St. Vincent and the Grenadines,
P.O. Box 1825, Villa, St. Vincent

Anti-Money Laundering Policy

Version: September 2017

Table of contents:

INTRODUCTION

The phrase “money laundering” covers all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source. **WBB CONSULTANCY SA** (“Company”) aims to detect, manage and mitigate the risks associated with money laundering and the financing of terrorism. The Company has introduced strict policy aimed on the detection, risk prevention or mitigation in respect of any suspicious activities performed by customers.

The Company is required to constantly monitor its level of exposure to the risk of money laundering and the financing of terrorism.

The Company believes that if it knows its client well and understands its instructions thoroughly, it will be better placed to assess risks and spot suspicious activities.

Политика по борьбе с отмыванием денег

Версия: Сентябрь 2017

Оглавление:

ВВЕДЕНИЕ

Фраза «отмывание денег» подразумевает любые процедуры, направленные на скрытие преступного источника происхождения средств, и представление их как происходящих из законного источника. **WBB CONSULTANCY SA** (далее – «Компания») стремится определить риски, связанные с отмыванием денег и финансированием терроризма, управлять его степенью и минимизировать последствия. В Компании введена строгая политика направленная на определение, предупреждение и минимизацию риска от любых подозрительных операций клиентов.

Компания в обязательном порядке постоянно осуществляет мониторинг уровня подверженности риску отмывания денег и финансирования терроризма.

Компания полагает, что тщательное изучение клиентов и их инструкций способствует лучшей оценке степени риска и обнаружению подозрительной активности.

1. CUSTOMER DUE DILIGENCE

1.1. Effective Customer Due Diligence (”CDD”) measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis. The customer identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.

1.2. During the Client’s Portal registration process an individual customers provide the following identification information to the Company:
a) Customer's full name;
b) Customer's date of birth;
c) Country of residence/location of customer;
d) Mobile telephone number and e-mail.

1.3. During the Client’s Portal registration process a corporate customers provide the following identification information to the Company:
a) Full company name;
b) Registration number and date;

c) Country of registration/incorporation;

d) Registered address;
e) Mobile telephone number and e-mail.

1.4. After receiving the identification information the Company’s staff should verify this information requesting the appropriate documents.

1.5. Appropriate documents for verifying the identity of customer include, but are not limited to, the following:

a) For an individual customer: A high resolution scanned copy or photo of pages of a passport or any other national ID, indicating family name and name(s), date and place of

1. ИЗУЧЕНИЕ КЛИЕНТОВ

1.1. Эффективная политика изучения клиентов является основным звеном управления риском отмывания денег и финансирования терроризма. Политика предполагает идентификацию клиента и верификацию его личности на основании документов и информации, как в момент начала обслуживания, так и постоянной основе.
Процедура идентификации и верификации требует сбора необходимых данных и проверку этой информации.

1.2. Во время процесса регистрации в Личном кабинете клиент, физическое лицо предоставляет Компании следующую информацию для идентификации:
a) Полное имя клиента;
b) Дату рождения клиента;
c) Страна резидентности и место пребывания;
d) Номер мобильного телефона и адрес электронной почты.

1.3. Во время процесса регистрации в Личном кабинете корпоративный клиент предоставляет Компании следующую информацию для идентификации:
a) Полное название корпоративного клиента;
b) Регистрационный номер и дату регистрации;
c) Страна регистрации или организации юридического лица;
d) Адрес регистрации;
e) Номер мобильного телефона и адрес электронной почты

1.4. После получения идентификационной информации персонал Компании проверяет эту информацию, запрашивая соответствующие документы.

1.5. Соответствующими документами для проверки идентификации клиента являются следующие (список не является исчерпывающим):
a) Для клиента, физического лица: Отсканированное в высоком разрешении изображение страниц паспорта либо другого документа удостоверяющего личность, которое включает Фамилию, Имя (Имена),

birth, passport number, issue and expiry dates, country of issue and Client's signature;

b) For a corporate customer: a high-resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, and, where applicable, Certificate of Change of Name, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

1.6. To verify proof of address of the customer the Company requires one of the following to be provided, in the same correct name of the customer:
a) A high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months;

b) A copy of a tax or rates bill from a local authority;
c) A copy of a bank statement (for a current account, deposit account or credit card account);
d) A copy of a bank reference letter.

1.7. When making a funds deposit or funds withdrawal via credit/debit card a customer is required to provide a scanned copy or photo of the credit/debit card (front and back side). The front side of credit/debit card should show the cardholder's full name, the expiry date and the first six and the last four digits of the card number (the rest of the digits may be covered). The copy or scan of the reverse side of credit/debit card should show the cardholder's signature, but the CVC2/CVV2 code must be masked.

1.8. If an existing customer either refuses to provide the information described above or if a customer has intentionally provided misleading information, the Company, after considering the risks involved, will consider closing any of an existing customer's account.

дату и место рождения, номер документа, дату выдачи и срок действия, страну, выдавшую документ, подпись клиента.
b) Для корпоративного клиента: Отсканированное в высоком разрешении изображение документа подтверждающего существование организации, например Сертификат об регистрации, и, при наличии, Сертификат о изменении имени, Сертификат подтверждающий легальный статус компании, Устав, лицензии выданные государственными органами (при наличии) и др.

1.6. Для проверки адреса клиента Компания требует предоставить один из следующих документов, который будет содержать тоже, корректное имя клиента:
a) Отсканированное в высоком разрешении изображение счета на оплату услуг (телефония, водоснабжение, газоснабжение, электроэнергия) не старше трёх месяцев;
b) Копия счета на оплату налоговых сборов либо пошлин от местного органа власти;
c) Копия выписки по банковскому счёту (текущий счёт, депозит либо карточный счёт);

d) Копия справки из банка о наличии счета.

1.7. При пополнении счета либо снятии средств со счета с помощью кредитной или дебитной карты клиенту необходимо предоставить отсканированное изображение кредитной/дебитной карты (лицевая и обратная сторона). Лицевая сторона карты должна содержать полное имя клиента, дату истечения действия, первые шесть и последние четыре цифры номера карты (остальные цифры должны быть скрыты). Изображение обратной стороны кредитной /дебитной карты должно содержать подпись картодержателя. Код CVC2/CVV2 должен быть скрыт.

1.8. В случае если, существующий клиент отказывается предоставить указанную выше информацию, либо клиент изначально предоставил неправильную информацию, Компания, после рассмотрения связанных с этим рисков, рассматривает необходимость закрытия любого существующего счета клиента.

1.9. The Regulations measures require further research and identification of customers who may pose a potentially high risk of money laundering/terrorism financing. If the Company has assessed that the business relationship with a customer pose a high risk it will apply the following additional measures:

a) Obtaining the information relating to the source of the funds or the wealth of the customer will be required (this will be done via e-mail or phone);
b) Seek further information from the customer or from Company's own research and third party sources in order to clarify or update the customer's information, obtain any further or additional information, clarify the nature and purpose of the customer's transactions with Company.

1.10. When obtaining information to verify the customer's statements about source of funds or wealth, the Company's staff will most often ask for and scrutinize details of the person's employment status or business/occupation. The Company's staff will ask for whatever additional data or proof of that employment/occupation that may be deemed necessary in the situation, particularly the appropriate confirming documents (employment agreements, bank statements, letter from employer or business etc.).

1.11. The Company will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. It particularly involves regularly reviewing and refreshing Company's view of what its customers are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the customer. It can also include anything that appears to be a material change in the nature or purpose of the customer's business relationship with Company.

1.9. Политики требуют дальнейшего изучения и идентификации клиентов, которые могут представлять потенциально высокий риск финансирования отмывания денег / финансирования терроризма. Если Компания оценит, что деловые отношения с клиентом представляют собой высокий риск, она будет предпринимать следующие дополнительные меры:
а) Собирать информацию, связанную с источниками средств клиента (по электронной почте либо телефону);

b) Собирать дополнительную информацию как от клиента так из собственных источников компании и сторонних лиц и организаций, чтобы уточнить, либо обновить, информацию о клиенте, получить любую дополнительную информацию, уточнить характер и цель операций клиента выполняемых с помощью/участием Компании.

1.10. При получении информации для проверки заявлений клиента об источнике средств сотрудники Компании чаще всего будут запрашивать и анализировать данные о трудоустройстве или бизнесе / профессии. Для подтверждения рода занятий / должности персонал Компании будет запрашивать любые дополнительные данные или доказательства, которые могут считаться необходимым в такой ситуации, в частности соответствующие подтверждающие документы (трудовые соглашения, банковские выписки, письма от работодателя или организации и т. д.).

1.11. Компания будет проводить постоянную проверку клиентов и мониторинг всех деловых отношений с клиентами. Это, в частности, предполагает регулярное рассмотрение и обновление взглядов Компании на деятельность клиентов, связанный с ними уровень риска, отсутствие противоречий с ранее предоставленной информацией. Также это может включать в себя все, что представляется существенным изменением характера или цели деловых отношений клиента с Компанией.

2. PAYMENTS POLICY

2.1. The Company's payments policy is governed by the Regulations for Non-Trading Operations, which is an inalienable part of Client Agreement and can be found on the Company Website.

3. PERSONNEL

AML Compliance Officer

3.1. The Company shall appoint an AML Compliance Officer, who will be fully responsible for the Company's AML and CFT program and report to the Board of the Company or a committee thereof any material breaches of the internal AML policy and procedures and of the Regulations, codes and standards of good practice.

3.2. AML Compliance Officer's responsibilities include:
a) Ensuring the Company's compliance with the requirements of the Regulations;

b) Establishing and maintaining internal AML program;

c) Establishing an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems;
d) Training employees to recognize suspicious transactions;
e) Receiving and investigating internal suspicious activity and transaction reports from staff and making reports to the FIU where appropriate;

f) Ensuring that proper AML records are kept;

g) Obtaining and updating international findings concerning countries with inadequate AML systems, laws or measures.

2. ПОЛИТИКА ПЛАТЕЖЕЙ

2.1. Политика платежей Компании регулируется Положением о неторговых операциях, которое является неотъемлемой частью Клиентского соглашения и может быть найдена на веб-сайте Компании.

3. ПЕРСОНАЛ

Специалист по финансовому мониторингу

3.1. Компания назначает специалиста по вопросам финансового мониторинга, который несёт полную ответственность за Программу противодействия отмыванию денег и финансированию терроризма и сообщает Правлению Компании о любых существенных нарушениях внутренней политики и процедур противодействия отмыванию денег и финансированию терроризма, а также нормативно-правовых документов, внутренних политик и корпоративных стандартов.

3.2. Ответственность специалиста по финансовому мониторингу включает:
a) Обеспечение соответствия Компании требованиям нормативно-правовых документов;
b) Разработка и обеспечение выполнения внутренней программы противодействия отмыванию денег и финансированию терроризма;
c) Разработка мероприятий по аудиту системы выполнения программы противодействия отмыванию денег и финансированию терроризма;
d) Проведение обучения сотрудников по выявлению подозрительных транзакций;
e) Проведение расследований по внутренним подозрительным операциям, проверка отчётов персонала о транзакциях, и предоставление отчётов в регулирующие органы, в случае необходимости;
f) Обеспечение надлежащего хранения информации по программе противодействия отмыванию денег и финансированию терроризма;
g) Создание и обновление списка стран, которые отнесены к странам с высоким риском нарушения программ

противодействия отмыванию денег и финансированию терроризма

Employees

3.3. All Company employees, managers and directors must be aware of this policy.

3.4. Employees, managers and directors who are engaged in AML related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML program must be reported in confidence to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee must report the violation to the Chief Executive Officer.

3.5. Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

Employee Training Programme

3.6. The Company provides AML training to employees who will be dealing with customers or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third party consultants.

3.7. Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies,

Сотрудники

3.3. Все сотрудники компании, включая руководящий состав, должны быть ознакомлены с данной политикой.

3.4. Сотрудники, и руководящий состав, в должностные обязанности которых входят вопросы по противодействия отмыванию денег и финансированию терроризма, при вступлении в должность, а также в дальнейшем на регулярной основе, должны пройти надлежащую проверку на наличие фактов привлечения к ответственности.
Любое нарушение этой политики или программы по противодействию отмыванию денег и финансированию терроризма должно быть доступны специалисту по финансовому мониторингу. В случае если это нарушение связанно с действиями специалиста по финансовому мониторингу сотрудник, обнаруживший нарушение, должен сообщить о нарушении Генеральному директору.

3.5. Сотрудники, в должностные обязанности которых входят вопросы по противодействия отмыванию денег и финансированию терроризма, должны проходить обучение по соблюдению этой политику и программы по противодействию отмыванию денег и финансированию терроризма. Обучение должно включать в себя мероприятия по определению рисков связанных с отмыванием денег и финансированием терроризма, а также обязательные действия, выполняемые после выявления рисков.

Программа обучения сотрудников

3.6. Компания проводит обучение сотрудников, которые связанны с обслуживанием клиентов, а также в должностные обязанности которых входят вопросы по противодействия отмыванию денег и финансированию терроризма. Компания может проводить обучение самостоятельно или привлекать внешних сторонних консультантов.

3.7. Каждый сотрудник компании имеет куратора, который проводит обучение всем политикам, процедурам, используемым

procedures, customer documentation forms and requirements, forex markets, trading platforms, etc. There is a training plan for each new employee and tests which are being held for 2-3 months (depending on level within the business).

формам и требованиям к документации клиентов, сведеньям о рынке маржинальной торговли, используемым торговым платформам и т.д.
Для каждого нового сотрудника разрабатывается план обучения. В течение 2-3 месяцев (в зависимости от занимаемой должности) проводится тестирование знаний.

3.8. The Company's AML training programmes is aimed to ensure its employees to receive appropriate training level with regards to any possible AML/TF risks.

3.8. Программы Компании по обучению вопросам противодействия отмыванию денег и финансированию терроризма направлены на то, чтобы обеспечить сотрудникам соответствующий уровень подготовки в отношении любых возможных рисков связанных с отмыванием денег и финансированием терроризма.

Content of training

Содержание обучения

3.9. The Company's AML and risk awareness training includes the following content:

3.9. Программы Компании по обучению вопросам противодействия отмыванию денег и финансированию терроризма и по обучению осведомлённости о риске включают в себя:

a) The Company's commitment to the prevention, detection and reporting of ML and TF crimes;

a) Обязательство Компании по предотвращению, выявлению и представлению отчётов по правонарушениям связанных с отмыванием денег и финансированием терроризма;

b) Examples of ML and TF that have been detected in similar organizations, to create an awareness of the potential ML and TF risks which may be faced by the Company's employees;

b) Примеры случаев отмывания денег и финансирования терроризма, которые были выявлены в аналогичных организациях, для обеспечения осведомлённости сотрудников о потенциальных рисках связанных с отмыванием денег и финансированием терроризма;

c) Well known or recognized typologies, especially where made available by the FATF or AML Supervisors;

c) Признаки подозрительных операций и типологии подозрительной активности, разработанные государственными регулирующими органами в сфере финансового мониторинга;

d) The consequences of ML and TF for the Company, including potential legal liability;

d) Возможные последствия для Компании, включая потенциальную юридическую ответственность, в случае нарушения требований по противодействию отмыванию денег и финансированию терроризма;

e) The responsibilities of the Company under the AML Act and Regulations;

e) Ответственность Компании согласно действующего законодательства;

f) Those particular responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Company's AML procedures.

f) Конкретная ответственность сотрудников, указанных в настоящей политике, и требования по соблюдению внутренних

g) How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.

h) The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").

WBB CONSULTANCY SA

процедур по противодействию отмыванию денег и финансированию терроризма.

g) Способы идентификации и действия в случае выявления необычной активности, которая может быть подозрительной транзакцией либо попыткой подозрительной транзакции.

h) Правила, которые применяются в случае незаконного раскрытия информации о обнаружении подозрительных транзакций.

WBB CONSULTANCY SA