ANTI - MONEY LAUNDERING AND COUNTER - TERRORISM FINANCING POLICY
(Version from 1/4/2015)

ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДЕНЕЖНЫХ СРЕДСТВ И ФИНАНСИРОВАНИЮ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ
(Редакция от 01.04.2015)

1. General terms

1.1. Anti - Money Laundering and Counter - Terrorism Financing Policy (hereafter – "AML/CTF Policy") is a constituent and integral part of the Customer agreement.

1.2. NPBFX Limited (hereafter – the "Company") strictly complies with the existing international legislation in the sphere of anti - money laundering and counter – terrorism financing.

1.3. As part of this AML/CTF Policy, the Company has established the "Know-Your-Customer" Policy that consists of constant analysis and monitoring of the Company's customer and his trading accounts transactions.

1.4. As part of this AML/CTF Policy, the Company has established the Refund Policy.

1.5. Main objectives of AML/CTF Policy are:

– establishment of the sustainable principles of AML/CTF Policy and their responsible fulfillment thereof to ensure timely disclose of the customers' criminal transactions on the trading accounts therefore (hence) reducing the influence on the compliant customers;

– ensuring the protection of business reputation of the Company;

– elimination of the involvement and participation of the Company's employees in money laundering and terrorism financing.

1.6. This AML/CTF Policy stipulates the general rules of the internal customer control and is binding for all employees of the Company.

1. Общие положения

1.1. Политика противодействия отмыванию денежных средств и финансированию террористической деятельности (далее – «Политика ПОД/ФТ») является составной и неотъемлемой частью Клиентского соглашения.

1.2. Компания NPBFX Limited (далее – «Компания») неукоснительно соблюдает действующее международное законодательство в области противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма.

1.3. В рамках данной Политики ПОД/ФТ в Компании утверждена Политика «Знай своего Клиента», выражающаяся в постоянном анализе и мониторинге Клиента Компании и его деятельности на торговых счетах.

1.4. В рамках данной Политики ПОД/ФТ в Компании утверждена Политика Возврата денежных средств.

1.5. Основными целями Политики ПОД/ФТ являются:

– создание сбалансированных принципов Политики ПОД/ФТ и разумное выполнение их таким образом, чтобы своевременно выявлять преступную деятельность Клиентов на своих торговых счетах, уменьшая при этом ее воздействие на законопослушных Клиентов;

– обеспечение сохранности деловой репутации Компании;

– исключение вовлечения и соучастия сотрудников Компании в процесс легализации доходов, полученных незаконным путем и финансирования терроризма.

1.6. Настоящая Политика ПОД/ФТ устанавливает общие правила внутреннего контроля Клиентов и обязательна к исполнению всеми сотрудниками Компании.

2. General Principles of Anti - Money Laundering and Counter - Terrorism Financing Policy

2.1. The Company does not open a trading account on an anonymous basis.

2.2. The Company has the right to block the access to Personal cabinet, suspend the trading activities on the accounts, cancel deposit/withdrawal requests, if in the course of collaboration with the Company any information is discovered that the Customer (for legal entities – the owner or director) is being involved in extremism, criminal activity or money laundering.

2.3. The Company shall under no circumstances accept cash as a deposit from the customers or pay cash to the customers.

2.4. Each customer of the Company shall use his/her personal e-wallet only for depositing/withdrawing of the funds. Thereby, the name of the e-wallet holder shall fully correspond to the name specified at the Customer's registration form on the Company's web-site.

2.5. Usage of the same payment accounts by different customers of the Company is (strictly) prohibited.

2.6. Each customer of the Company must verify his/her e-wallet payment details in his/her Trader's Room, to be able to use them for performing (to perform) deposit and withdrawal transactions.

2.7. In case any doubt arises regarding the validity and relevance of the Customer's payment details, the Company has the right to request a screenshot of the payment system page that contains information about its (this e-wallet) holder.

2.8. Internal transfer of the funds between the accounts within the Company may be performed by the verified Customer only. Funds transfer between the accounts/Trader's rooms belonged to different Customers of the Company is prohibited.

2. Общие принципы Политики противодействия отмыванию денежных средств и финансированию террористической деятельности

2.1. Компания не осуществляет открытие торгового счета на анонимного владельца.

2.2. Компания имеет право заблокировать вход в Личный кабинет, приостановить торговую деятельность на счетах, либо отменить заявку на ввод/вывод денежных средств, если в процессе взаимодействия Клиента (для юридических лиц: владельцев или директоров) с Компанией появляются сведения об участии Клиента (представителей компании) в экстремистской деятельности или деятельности, связанной с отмыванием денежных средств.

2.3. Компания не принимает наличные деньги от Клиентов в качестве депозита и не выплачивает наличные деньги ни при каких обстоятельствах.

2.4. Каждый Клиент Компании должен использовать для зачисления/снятия денежных средств электронный кошелек, принадлежащий только ему. При этом имя держателя электронного кошелька должно полностью соответствовать имени, указанному при регистрации Клиента на сайте Компании.

2.5. Использование одних и тех же платежных реквизитов разными Клиентами Компании запрещено.

2.6. Каждый Клиент Компании обязан верифицировать платежные реквизиты своих электронных кошельков в Личном Кабинете, которые он намерен использовать для осуществления операций по вводу и выводу средств.

2.7. В случае возникновения сомнений в достоверности и актуальности полученных данных о платежных реквизитах Клиента, Компания в праве запросить снимок экрана компьютера (screen shot), на котором открыта Интернет-страница платежной системы с размещенными на ней сведениями о владельце данного электронного кошелька.

2.8. Денежные средства внутри Компании могут переводиться только между счетами Клиента, прошедшего процедуру верификации личных данных. Перевод денежных средств меду счетами и/или лицевыми счетами, принадлежащими разным Клиентам Компании, запрещен.

2.9. Funds may be withdrawn only by the same way and using the same payment account (details), via which such funds have been deposited to the account, unless otherwise is stipulated by the Company's regulations.

2.9. Денежные средства могут быть выведены только тем же способом и на те же реквизиты, с которых осуществлялся их ввод, если иное не предусмотрено правилами Компании.

2.10. The Company shall carry out mandatory customer verification according to the Customer Agreement and in conformity with the principles of the "Know-Your-Customer" Policy.

2.10. Компания проводит обязательную верификацию Клиентов согласно Клиентскому соглашению и в соответствии с принципами Политики «Знай своего Клиента».

3. Furnishing of information to Authorized authority

3. Предоставление сведений в Уполномоченный орган

3.1. In case of detection of any suspicious activity carried out by the Customer on his/her trading accounts, Company's employee must inform and provide all the necessary documents to the Compliance Manager.

3.1. При обнаружении подозрительной деятельности, осуществляемой Клиентом на своих торговых счетах, сотрудник Компании обязан уведомить об этом Комплаенс Менеджера и направить ему все необходимые документы.

3.2. Each employee of the Company shall inform the Compliance Manager of any suspicious proposals made by customers even if the transactions don't take place.

3.2. Каждый сотрудник компании обязан сообщать о любых подозрительных предложениях Клиентов, даже если операция не была проведена, Комплаенс Менеджеру.

3.3. All the actions taken in relation to the transactions to be communicated to the authorized authority shall be documented and kept in compliance with the established requirements of confidential information protection.

3.3. Все действия, предпринятые в связи с операциями, сообщения о которых подлежат предоставлению в уполномоченный орган, подлежат документированию и хранятся с соблюдением установленных требований по обеспечению сохранности конфиденциальной информации.

3.4. Details of the transactions to be communicated to the authorized authority and any contacts with the authorized authorities regarding such transactions shall be documented.

3.4. Детали операций, сведения о которых подлежат предоставлению в уполномоченный орган, а также любые контакты с уполномоченными органами в отношении этих операций, документируются.

4. Confidentiality

4. Конфиденциальность

4.1. Information about the customers and their transactions obtained according to the AML/CTF Principles is confidential.

4.1. Информация о Клиентах и их операциях, полученная в рамках принципов Политики ПОД/ФТ, является конфиденциальной.

4.2. The Company employees and the Compliance Manager shall not be entitled to inform the customers or other persons of forms, methods and implementation ways of the AML/CTF Policy.

4.2. Сотрудники Компании и Комплаенс Менеджер не вправе информировать Клиентов и иных лиц о формах, способах и методах осуществления принципов Политики ПОД/ФТ.

4.3. Disclosure to other persons of any information that the Company has furnished to the authorized authority and any data concerning the customer's transactions or activities shall be strictly prohibited.

4.3. Раскрытие иным лицам информации о том, что Компанией были представлены в уполномоченный орган сведения об операциях или деятельности Клиента, строго запрещается.

5. Documents and information storage

5. Хранение документов и информации

5.1. Data obtained as a result of the customer identification and information about the transactions

5.1. Данные, полученные в результате идентификации Клиентов, и сведения об операциях

shall be kept as the evidence of measures taken by the Company in accordance with the applicable AML/CTF Policy, in order to be used as the evidence in the course of investigations held by authorized authorities.

хранятся как доказательство предпринятых Компанией в соответствии с действующей Политикой ПОД/ФТ мер, а также для их использования в качестве доказательств при проведении расследования уполномоченными органами.

5.2. Customers' ID information shall be kept for at least five years after the termination of business relations with the customer according to the applicable "Know-Your-Customer" Policy.

5.2. Идентификационные данные Клиентов подлежат хранению в течение не менее пяти лет после прекращения отношений с Клиентом в соответствии с действующей Политикой «Знай своего Клиента».

5.3. Data on the transactions communicated to authorized authority shall be kept for at least five years after the transaction date.

5.3. Данные об операциях, сведения по которым были направлены в уполномоченный орган, подлежат хранению в течение не менее пяти лет с даты совершения операции.

5.4. All internal and external reports furnished as part of implementation of the AML/CTF Policy shall be kept for at least five years after the report submission.

5.4. Все внутренние и внешние отчеты, полученные в рамках реализации принципов Политики ПОД/ФТ, подлежат хранению в течение не менее пяти лет с даты представления отчета.

5.5. The Company is obligated to keep information about all its actions taken to fulfill the requirements to collect from employees, and transfer to the authorized authority about detected transactions. If it is decided not transfer the information about suspected money laundering/counter-terrorism financing to the authorized authority, information concerning such facts shall also be subject to keeping.

5.5. Компания обязана хранить информацию обо всех действиях, предпринятых в связи с выполнением требований о получении от работников и представлении в уполномоченный орган сведений о выявленных операциях. В том случае, если принято решение не направлять в уполномоченный орган сведения относительно возможного отмывания денежных средств/финансирования терроризма, информация о данных фактах все равно подлежит хранению.