ООО «Альпари Евразия»

Alpari Evrasia LLC

AML & Payments Policy

Политика платежей и ПОД/ФТ

GENERAL PROVISIONS

Anti-Money Laundering Policy ("Policy") is an integral part of the Policy of Internal Control of Alpari Eurasia LLC ("Company") approved by the Head of the Company and developed in accordance with Decree of the President of the Republic of Belarus No. 231, dated the 4th of June, 2015 "On Carrying out Activities in the Over-the-counter Forex Market", Resolution of the Board of the National Bank of the Republic of Belarus No. 69, dated the 12th of February, 2016 "On approval of the Instruction on Setting Requirements to Organising Internal Control and Risk Management in Forex Companies, the National Forex Centre", Law of the Republic of Belarus No. 165-3, dated the 30th of June, 2014 "Actions to be taken to prevent legitimisation of the proceeds of crime and the financing of terrorism and financing the proliferation of weapons of mass destruction", other legal acts and taking into account the results of the National Risk Assessment in the Republic of Belarus and the Risk Assessment Report of the Company dated the 14th of February, 2019.

The Company's Internal Control System in AML / CFT is organised within the Company's overall internal control system and the Company's risk management system and ensures the prevention of the Company's intentional or unwitting involvement in the ML / FT process. The Company has approved and implemented the Internal Control Policy and Internal Control Rules, and there is an Internal Control Department that complies with the requirements of the legislation of the Republic of Belarus. The Company has introduced a strict policy aimed at the detection, prevention, and mitigation of any risks in respect of any suspicious activities performed by clients.

The Internal Control System in AML/CFT is implemented in the following main directions:

- identification and verification, in cases stipulated by law, of all the Company's clients engaged in financial transactions, and the monitoring of their activities during the servicing process;
- identifying, documenting of suspicious transactions and reporting to the Financial Monitoring Authority (Financial Intelligence Unit);
- record-keeping of transactions, information, and documents (copies) for the period established by law (for at least five years).

The Company regularly identifies, assesses, and implements measures to minimise its risk of exposure to money laundering and the financing of terrorism, and based on this assessment, applies a risk-oriented approach to ensure that measures to prevent or mitigate money laundering and the financing of terrorism are commensurate with the risks identified.

CUSTOMER DUE DILIGENCE

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

The Company doesn't keep anonymous accounts or accounts with obviously fictitious names.

Effective Customer Due Diligence ("CDD") measures are essential to the management of risks associated with money laundering and financing terrorism. CDD means identifying the customer and verifying their true identity on the basis of documents, data, or other

information both at the moment of starting a business relationship with the customer and on an ongoing basis. The customer identification and verification procedures require, firstly, the collection of data, and secondly, attempts to verify that data.

During the my.alpari.by registration process, individual customers provide the following identification information to the Company:

- Full name: surname, first name, patronymic (if any);
- Date and place of birth;
- Place of residence and/or place of stay;
- Citizenship;
- Mobile telephone number and email;
- Details of the passport/ID;
- Information on the beneficiary (when applicable).

During the my.alpari.by registration process, corporate customers provide the following identification information to the Company:

- Full company name;
- Registration number and date of the state registration of the customer organisation, name of the registration authority (if any);
- Country of registration/incorporation;
- Tax number or other identification number (for non-residents);
- Principal place of business;
- Surname, first name, patronymic (if any) of the head (other person authorised under constituent documents to act in the name of such customer organisation), of a person who manages business accounting, and/or of other officials duly authorised by their head or by law to act in the name of the customer organisation. Should a legal entity (management company) act as a head, data provided by this part shall be recorded;
- Data on beneficiary owners and (should the identification measures fail to reliably identify the beneficiary owner) data on the person who fulfils functions of a sole executive body of the customer organisation or a person who heads its collective executive body;
- Collectives of founders (partners, members) holding at least 10 percent of the shares (stakes in the authorised capital, units) in the organisation; their shareholdings (number of stakes in the authorised capital, units) in the organisation;
- Structure of management bodies;
- Types of activities;
- Purpose of maintaining relations and intended type of relations with the Company.
- Mobile telephone number and email.

After receiving the identification information, the Company's staff should verify this information by requesting supporting documentation.

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

- For an individual customer: A high-resolution photo of the customer with a passport or any other national ID opened to the page that displays their full name, date and place of birth, passport number, issue and expiry dates, country of issue, signature, and photo;

- For a corporate customer: a high-resolution copy of documents showing the existence of the entity, such as a 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.

Individual customers can also go through the Web-ID procedure via video call. Then, the customer shall also provide a high-resolution scanned copy or photo of pages of a passport or any other national ID, indicating their full name, date and place of birth, passport number, issue and expiry dates, country of issue, and Client's signature.

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 high-resolution copy of a utility bill (landline phone, water, electricity) issued within the last 3 months;
- A copy of a tax or rates bill from a local authority;
- A copy of a bank statement (for a current account, deposit account, or credit card account);
- A copy of a bank reference letter.

When making a funds deposit or funds withdrawal via credit/debit card, customers are 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 must 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 covered.

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 the existing customer's account.

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 a business relationship with a customer poses a high risk, it will apply the following additional measures:

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

When obtaining information to verify the customer's statements about the source of funds or wealth, the Company's staff will most often ask for and scrutinise 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 supporting documents (employment agreements, bank statements, letter from employer or business etc.).

The Company will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. In particular, this involves regularly reviewing and

updating the 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.

PAYMENTS POLICY

The Company's payments policy is governed by the Terms of Transactions and Client Agreement, which can be found on the "Regulatory Documents and Staff" page located in the "Trading terms" section on the Company website (www.alpari.by)

Payment for margin requirements by bank payment cards, providers ASSIST (https://www.belassist.by) and WEBPAY (https://www.webpay.by):

We accept cards issued by international payment systems Visa, MasterCard, payment system BELKART.

The card data is routed to the bank's secure authorization page. To make a payment, enter the card details: number, cardholder, expiration date and the three-digit security code. The three-digit security code (CVV2 for Visa, CVC2 for MasterCard) is the three digits printed on the back of the card if the card supports 3DSecure technology. For cardholders of the BELKART payment system, the Internet password is the same as the three-digit security code.

After entering the card details, you will be redirected to the page of the bank that issued the card and asked to enter the security code.

The personal information you provide (for example: name, address, phone number, email, bank card number, etc.) is confidential and not subject to disclosure. Card data is transmitted only in encrypted form and is not stored on the Company's website.

After making a payment via a bank card, it is necessary to keep card receipt (confirmation of your payment) for reconciliation with an extract from the card account (for approving transactions in case of disputes).

In case of failed transaction you should contact (technical support service) our specialists via Telegram messenger, via online-chat, by Email operations@alpari.by or call the number +375 (17) 388-05 -08.

Margin requirements are recorded in the Client's account anywhere from 1 minute to 1 hour from the time when funds are deposited. In exceptional cases, the processing company or employees of the Company's internal control department may decide to audit your transaction. In this case, the timeframe for crediting funds could take up to three days. Transactions fees, reimbursable costs (if applicable), and transaction limits are posted in the Company's website in the sections "Deposit and withdrawal methods", "Terms of transactions", and "Conditions of Forex trading terms", as well as in the corresponding section of the MyAlpari page. The Company provides refunds only in exceptional cases and at the customer's request by emailing operations@alpari.by, including the application and other documents justifying such a refund (e.g. failure to provide services, erroneous transfer, etc.). Cash refunds are not allowed when a credit card is used for payment. Refunds will be

made within seven calendar days from the date when the application is received. The refund amount will be equal to (but not exceed) the funding amount. Margin requirements are refunded in accordance with standard procedure and in the ways indicated in the relevant sections of the Company's website. The payment via bank card is refunded to the payment card that was used for that payment.

The company does not provide financial services to residents of the United States or its territories, Canada, Iran, North Korea, Afghanistan, Bosnia and Herzegovina, Ethiopia, Laos, Syria, Yemen, Algeria, Ecuador, Indonesia, Myanmar, Morocco, Nicaragua, Pakistan, Panama, Senegal, Zimbabwe, Trinidad and Tobago, Albania, or Barbados. In addition, visiting this site, using the services, paying or attempting to pay with a bank payment card issued by your bank may be illegal (prohibited) actions in the country where you are located, regardless of your citizenship or nationality, and may result in liability as envisaged in local laws.

PERSONNEL

AML Compliance Officer

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 Director any material breaches of the internal AML policy and procedures and of the Regulations, codes and standards of good practice.

The AML Compliance Officer's responsibilities include:

- organising customer identification;
- organising risk management procedures related to the consequences of the actions of third parties with regards to AML/CFT;
- making decisions on the recognition of a financial transaction as suspicious (or unsuspicious) and submission of information about it to the to the Financial Monitoring Authority (Financial Intelligence Unit), as well as decisions on further action with respect to the client;
- making decisions on suspension (renewal) of a financial transaction in cases provided for by legislative acts;
- making decisions on the refusal to execute a contract for carrying out operations with non-deliverable over-the-counter financial instruments (client agreement) in writing in cases provided for by legislative acts;
- signing by electronic digital signature of special forms sent to the Financial Intelligence Unit in the form of an electronic document;
- checking the correctness and completeness of special forms filled out by the Company's employees, as well as the timeliness of their submission to the Financial Intelligence Unit;
- organising follow-up control in order to identify suspicious financial transactions of a long-term nature and not determined at the stage of current control as subject to special monitoring;
- examination of the knowledge of employees of the Company's structural units within the organizational structure of the internal control system for preventing the legalisation of criminally obtained income, financing terrorist activities, and financing the proliferation of weapons of mass destruction;

- other functions stipulated by the Rules of internal control in terms of AML / CFT.

Employees

All Company employees, managers, and directors must be aware of this policy and the Rules of internal control.

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.

Employees 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 Program

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.

Each person employed within the Company is assigned a supervisor who teaches them in relation to all policies, procedures, customer documentation forms and requirements, forex markets, trading platforms, etc. There is a training plan for each new employee and tests which are held over 2-3 months (depending on their level within the business).

The Company's AML training programs are aimed to ensure its employees receive the appropriate level of training with regards to any possible AML/TF risks.

Content of training

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

- The Company's commitment to the prevention, detection, and reporting of ML and TF crimes.
- Examples of ML and TF that have been detected in similar organisations, to raise awareness of the potential ML and TF risks that may be faced by the Company's employees
- Well known or recognised typologies, especially where made available by the FATF.
- The consequences of ML and TF for the Company, including potential legal liability.
- The responsibilities of the Company under the AML Act and Regulations.
- The specific responsibilities of employees as identified in this AML Policy, and regulations for employee compliance with the Company's AML procedures.
- How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
- The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").

ОБЩИЕ ПОЛОЖЕНИЯ

Политика в области ПОД/ФТ («Политика») является составной частью Политики внутреннего контроля ООО «Альпари Евразия» («Компания»), утвержденной руководителем Компании и разработанной в соответствии с Указом Президента Республики Беларусь от 4 июня 2015 г. N 231 «Об осуществлении деятельности на внебиржевом рынке Форекс», Постановлением Правления Национального банка Республики Беларусь от 12.02.2016 N 69 «Об утверждении Инструкции об установлении требований к организации внутреннего контроля и управления рисками в форекс-компаниях, Национальном форекс-центре», Закона Республики Беларусь от 30 июня 2014 г. №165-З «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения», иными законодательными актами и с учетом итогов Национальной оценки рисков в Республике Беларусь и Отчете об оценке рисков в ООО «Альпари Евразия» от 14.02.2019.

Система внутреннего контроля Компании в сфере ПОД/ФТ организуется в рамках общей системы внутреннего контроля Компании и системы управления рисками Компании и обеспечивает недопущение умышленного или невольного вовлечения Компании в процесс ОД/ФТ. В компании утверждены и выполняются Политика внутреннего контроля, Правила внутреннего контроля, существует отдел внутреннего контроля, что соответствует требованиям законодательства Республики Беларусь. Компания ввела строгую политику, направленную на выявление, предотвращение и снижение рисков в отношении любых подозрительных действий, совершаемых клиентами.

Система внутреннего контроля в области ПОД/ФТ реализуется по следующим основным направлениям:

- идентификация и верификация в случаях, предусмотренных законодательством, всех клиентов Компании, осуществляющих финансовые операции, мониторинг их деятельности в процессе обслуживания;
- выявление, документальное фиксирование финансовой операции, подлежащей особому контролю, и передача соответствующих сведений в орган финансового мониторинга (финансовой разведки);
- хранение сведений и документов (их копий) в течение срока, установленного законодательством (как минимум в течение 5 лет).

Компания регулярно определяет, оценивает и принимает меры по снижению собственных рисков вовлечения в процессы отмывания денег и финансирования терроризма и на основе этой оценки применяет риск-ориентированный подход для того, чтобы меры по предупреждению отмывания денег и финансирования терроризма соответствовали выявленным рискам.

НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТОВ

Компания считает, что, если она хорошо знает своего клиента и хорошо понимает его инструкции, у нее будет больше возможностей для оценки рисков и выявления подозрительных действий.

Компания не ведет анонимные аккаунты или аккаунты, открытые на явно вымышленные имена.

Эффективные меры по надлежащей проверке клиентов («НПК») необходимы для управления риском отмывания денег и финансирования терроризма. НПК означает идентификацию клиента и проверку его подлинной личности на основе документов и иной информации как при установлении деловых отношений, так и на постоянной основе. Процедура идентификации клиента и верификации сведений по клиенту требуют, во-первых, сбора данных и, во-вторых, действий по проверке этих данных.

В процессе регистрации личного кабинета клиента my.alpari.by клиенты-физические лица представляют Компании следующие идентификационные сведения:

- фамилия, собственное имя, отчество (при наличии);
- дата и место рождения;
- место жительства и (или) место пребывания;
- гражданство;
- номер телефона и e-mail;
- реквизиты паспорта или иного документа, удостоверяющего личность;
- сведения о выгодоприобретателе (при наличии таких сведений).

В процессе регистрации личного кабинета клиента my.alpari.by клиенты-юридические лица предоставляют Компании следующие идентификационные сведения:

- наименование;
- регистрационный номер и дату государственной регистрации клиента-организации, наименование регистрирующего органа (при их наличии);
- место нахождения;
- страна регистрации;
- учетный номер плательщика, для нерезидентов – иной идентификационный номер;
- основное место деятельности;
- фамилию, собственное имя, отчество (при наличии) руководителя (иного лица, уполномоченного в соответствии с учредительными документами действовать от имени клиента-организации), лица, осуществляющего руководство бухгалтерским учетом, и (или) иных уполномоченных должностных лиц, которым законодательством или руководителем предоставлено право действовать от имени этой организации. В случае, если в качестве руководителя выступает юридическое лицо – управляющая организация, фиксируются данные, предусмотренные настоящей частью;
- сведения о бенефициарных владельцах, а если в результате принятия мер по идентификации клиента бенефициарный владелец достоверно не установлен – сведения о лице, осуществляющем функции единоличного исполнительного органа клиента-организации, либо лице, возглавляющем ее коллегиальный исполнительный орган;
- состав учредителей (участников, членов), владеющих не менее чем 10 процентами акций (долей в уставном фонде, паев) организации; доли их владения акциями (размер доли в уставном фонде, паев) организации; структуру органов управления;
- виды деятельности;

- цели установления и предполагаемый характер отношений с Компанией;
- номер телефона и e-mail.

После получения информации при идентификации сотрудники Компании должны проверить эту информацию, запросив соответствующие документы.

Такие документы для проверки включают, помимо прочего, следующие:

- для клиента-физического лица: фотографии клиента в высоком разрешении с паспортом или любым другим национальным удостоверением личности, открытым на разворотах, содержащих фамилию, имя и отчество клиента, дату и место рождения, номера паспорта / личного номера, дату выдачи и истечения срока действия документа, подпись и фото клиента, прописку (регистрацию);
- для клиента-организации: копия документов в высоком разрешении, подтверждающих существование организации, таких как свидетельство о регистрации, свидетельство об изменении наименования, выписка из торгового реестра, устав, лицензия (если применимо) и другие документы.

Клиент-физическое лицо также может пройти процедуру Web-ID (веб-идентификации) посредством видеозвонка. Затем клиент также должен представить скан-копию в высоком разрешении или фотографию паспорта или любого другого национального удостоверения личности с указанием фамилии, имени и отчества, даты и места рождения, номера паспорта, даты выдачи и срока действия, страны выдачи, фотографии и подписи клиента, прописки (регистрации).

Для проверки подтверждения адреса регистрации (жительства) клиента требуется представление одного из следующих документов, выданных на имя клиента:

- копия счета за коммунальные услуги (стационарный телефон, вода, электричество) в высоком разрешении за последние 3 месяца;
- копия счета о налогах или налоговых ставок от местного органа власти или налоговой инспекции;
- копия банковской выписки;
- копия информационного (рекомендательного) письма.

При внесении маржинального обеспечения (внесении средств) или возврата маржинального обеспечения (вывода средств) с помощью банковской платежной карты клиент должен представить отсканированную копию или фотографию банковской карты (лицевая и оборотная стороны). На лицевой стороне карты должно быть указано полное имя клиента-владельца карты, срок действия и первые шесть и последние четыре цифры номера карты (остальные цифры могут быть закрыты). Копия обратной стороны карты должна содержать подпись владельца, а код CVC2/CVV2 должен быть скрыт.

Если клиент отказывается представить информацию, указанную выше, либо если клиент преднамеренно представил вводящую в заблуждение информацию, Компания, рассмотрев связанные с этим риски, рассматривает вопрос о закрытии учетной записи клиента.

Меры, указанные в законодательстве и регламентах Компании, требуют дальнейшего изучения и выявления клиентов, которые могут представлять потенциально высокий риск отмывания денег и финансирования терроризма. Если Компания

оценила, что деловые отношения с клиентом представляют высокий риск, она будет применять следующие дополнительные меры:

- требования представить информацию, касающуюся источника происхождения средств клиента (по электронной почте или по телефону);
- запрос дополнительной информации у клиента или из собственных и сторонних источников Компании, чтобы уточнить или обновить информацию о клиенте, получить любую дополнительную информацию, уточняющую характер и цель операций клиента с Компанией.

При получении информации для проверки сведений, полученных от клиента, об источнике происхождения средств сотрудники Компании запрашивают и тщательно изучают сведения о статусе занятости или сфере деятельности (профессии) клиента. Персонал Компании запрашивает любые дополнительные данные или доказательства профессии и рода занятий, которые могут быть сочтены необходимыми в данной ситуации, особенно подтверждающие документы (трудовые договоры, банковские выписки, письма от работодателя и т.д.).

Компания проводит постоянную экспертизу клиентов и мониторинг аккаунтов в рамках деловых отношений с клиентом. Это, в частности, включает регулярный пересмотр и обновление представления Компании о том, что делают ее клиенты, об уровне риска, который они представляют, и о том, не противоречит ли что-либо информации или мнениям, которые были получены ранее о клиенте. Сюда может также входить все, что представляется существенным изменением характера или цели деловых отношений клиента с Компанией.

ПОЛИТИКА ПЛАТЕЖЕЙ

Политика платежей Компании регулируется Правилами совершения операций и Соглашением о совершении операций, которые можно найти на странице «Документы и кадровая информация», расположенной в разделе «Условия Форекс операций» на веб-сайте Компании www.alpari.by.

Внесение маржинального обеспечения банковскими платежными картами, провайдеры ООО «Компания электронных платежей «АССИСТ» (https://www.belassist.by) и ООО «ВЕБ ПЭЙ» (https://www.webpay.by):

К оплате принимаются карты международных платежных систем VISA, MasterCard, платежной системы БЕЛКАРТ. Безопасность совершения платежа обеспечивается современными методами проверки, шифрования и передачи данных по закрытым каналам связи.

Ввод данных карты осуществляется на защищенной авторизационной странице банка. Для оплаты необходимо ввести реквизиты карты: номер, имя держателя, срок действия и трехзначный код безопасности. Трёхзначный код безопасности (CVV2 для VISA, CVC2 для MasterCard) — это три цифры, находящиеся на обратной стороне карты, если карта поддерживает технологию 3DSecure. Для держателей карт платежной системы БЕЛКАРТ эквивалентом трехзначного кода безопасности является интернет-пароль.

После введения реквизитов карты вы будете перенаправлены на страницу банка, выпустившего карту, для ввода кода безопасности.

Предоставляемая вами персональная информация (например: имя, адрес, телефон, e-mail, номер банковской карты и прочее) является конфиденциальной и не подлежит разглашению. Данные карты передаются только в зашифрованном виде и не сохраняются на веб-сайте Компании.

После совершения оплаты с использованием банковской карты необходимо сохранять полученные карт-чеки (подтверждения об оплате) для сверки с выпиской из карт-счёта (с целью подтверждения совершённых операций в случае возникновения спорных ситуаций).

В случае, если не удалось провести платёж, Вам необходимо обратиться (в службу технической поддержки) к нашими специалистами в чате мессенджера Telegram, в онлайн-чате, по e-mail operations@alpari.by или по номеру телефона +375 (17) 388-05-08.

Отражение маржинального обеспечения на аккаунте Клиента осуществляется от 1 минуты до 1 часа с момента проведения операции по внесению денежных средств. В исключительных случаях процессинговая компания или сотрудники отдела внутреннего контроля Компании могут инициировать проверку вашей операции. В этом случае срок зачисления может составить до трех дней. Комиссии и компенсируемые издержки (в случае их установления), лимиты на совершение транзакций указаны на сайте Компании в разделах «Способы пополнения и вывода», «Условия совершения операций», «Условия Форекс-операций», а также в соответствующем разделе Личного кабинета.

Возврат средств операцией Refund может быть осуществлен Компанией в исключительных случаях по запросу клиента с представлением на почтовый адрес operations@alpari.by заявления и иных документов, обосновывающих такой возврат (факт неоказания услуги, ошибочное зачисление и др.). При оплате банковской картой возврат наличными денежными средствами не допускается. Возврат денежных средств будет осуществлен в течение 7 календарных дней со дня получения заявления. Сумма возврата будет равняться (не превышать) суммы пополнения. Возврат маржинального обеспечения в нормальном режиме осуществляется способами, указанными на сайте Компании в соответствующих разделах. При оплате банковской платёжной картой возврат денежных средств осуществляется на карточку, с которой была произведена оплата.

Компания не оказывает финансовые услуги резидентам США и территорий, Канады, Ирана, КНДР, Афганистана, Боснии и Герцеговины, Эфиопии, Лаоса, Сирии, Йемена, Алжира, Эквадора, Индонезии, Мьянмы, Марокко, Никарагуа, Пакистана, Панамы, Сенегала, Зимбабве, Тринидада и Тобаго, Албании, Барбадоса. Кроме того, посещение этого сайта, пользование услугами, оплата или попытка оплаты банковской платежной картой, выпущенной вашим банком, могут быть незаконными (запрещенными) действиями на территории страны, где вы находитесь, вне зависимости от вашего гражданства или подданства, и могут повлечь установленную местными законами ответственность.

ПЕРСОНАЛ

Сотрудник, ответственный за соблюдение правил внутреннего контроля

Компания назначает ответственного за соблюдение правил внутреннего контроля, в том числе в сфере ПОД/ФТ, который несет полную ответственность за осуществление мер по ПОД/ФТ в Компании и сообщает руководителю о любых нарушениях внутренней политики и процедур ПОД/ФТ, а также иных положений, законов, стандартов практики и др.

В обязанности такого сотрудника входит следующее:

- организация проведения идентификации клиентов;
- организация процедур управления рисками, связанными с возможностью пострадать от деятельности сторонних лиц по легализации доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения;
- принятие решения о признании финансовой операции подозрительной (неподозрительной) и предоставлении сведений о ней в орган финансового мониторинга, а также решения о дальнейших действиях в отношении клиента;
- принятие решения о приостановлении (возобновлении) финансовой операции в случаях, предусмотренных законодательными актами;
- принятие решения об отказе в исполнении договора на осуществление операций с беспоставочными внебиржевыми финансовыми инструментами (клиентского соглашения) в письменной форме в случаях, предусмотренных законодательными актами;
- подписание электронной цифровой подписью отправляемых в орган финансового мониторинга специальных формуляров в виде электронного документа;
- проверка правильности и полноты заполнения сотрудниками Компании специальных формуляров, а также своевременности их представления в орган финансового мониторинга;
- организация последующего контроля с целью выявления подозрительных финансовых операций, носящих длительный характер и не определяемых на стадии текущего контроля как подлежащих особому контролю;
- проверка знаний сотрудников структурных подразделений Компании, входящих в организационную структуру системы внутреннего контроля, в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;
- иные функции, предусмотренные Правилами внутреннего контроля в части ПОД/ФТ.

Сотрудники Компании

Все сотрудники, менеджеры и директор Компании должны изучить эту политику и Правила внутреннего контроля. Сотрудники Компании, выполняющие обязанности, связанные с ПОД/ФТ, должны пройти соответствующую проверку. Эта проверка включает в себя установление фактов привлечения сотрудника к уголовной ответственности, проводимое при приеме на работу, и контроль во время работы. О

любом нарушении политики и Правил внутреннего контроля необходимо в конфиденциальном порядке сообщить сотруднику, ответственному за осуществление внутреннего контроля, если только такое нарушение не затрагивает самого ответственного сотрудника, и в этом случае сотрудник должен сообщить о нарушении директору Компании.

Сотрудники должны быть обучены тому, как соблюдать эту политику и Правила внутреннего контроля. Это включает в себя готовность к риску отмыванию денег и финансированию терроризма и знание того, что делать, когда такие риски выявлены.

Программа обучения (инструктажа) сотрудников

Компания предоставляет соответствующее обучение (инструктаж) сотрудникам, которые будут иметь дело с клиентами или будут участвовать в любых процессах проверки, верификации или мониторинга. Компания может проводить инструктаж по месту нахождения Компании в том числе с привлечением сторонних консультантов.

Каждому сотруднику, работающему в Компании, назначается руководитель, который обучает его в отношении всех политик, процедур, форм и требований к документам клиента, рынков Форекс, платформ и т.д. Для каждого нового сотрудника существует план обучения и тесты, которые проводятся в течение 2-3 месяцев.

Программа инструктажа Компании по ПОД/ФТ направлена на то, чтобы обеспечить своим сотрудникам соответствующий уровень подготовки в отношении любых возможных рисков, связанных с ОД/ФТ.

Содержание инструктажа

Инструктаж по ПОД/ФТ и управлению рисками помимо прочего включает в себя следующее:

- деятельность Компании по предотвращению, выявлению и сообщению о преступлениях в сфере ОД/ФТ;
- примеры ОД/ФТ, обнаруженные в аналогичных организациях, для повышения осведомленности о потенциальных рисках ОД/ФТ, с которыми могут столкнуться сотрудники Компании;
- хорошо известные или признанные типологии, особенно в тех случаях, когда они предоставлены FATF (типологические отчеты);
- последствия ОД/ФТ для Компании, включая потенциальную юридическую ответственность;
- обязанности Компании согласно Закону №165-З и иным положениям и Правилам внутреннего контроля;
- конкретные обязанности сотрудников, которые определены в настоящей политике и Правилах внутреннего контроля, и регламентация соблюдения сотрудниками процедур внутреннего контроля Компании;
- как выявлять и сообщать о необычной активности, которая может быть подозрительной транзакцией или попыткой транзакции (критерии);
- правила, применяемые против раскрытия (сообщения клиенту) информации о подозрительных финансовых операциях.