ПОЛИТИКА

Политика противодействия легализации преступных доходов и финансированию терроризма (AML/CFT)

Anti-Money Laundering & Counter-Terrorism Financing Policy

Компания	Free Bird PSP L.L.C-FZ
Код документа	[02-000]
Версия	1.1
Дата утверждения	06.10.2026
Владелец документа	MLRO
Периодичность пересмотра	Ежегодно или при изменении законодательства
Классификация	Конфиденциально (Confidential)
Контакты	ceo.freebird@gmail.com

Дубай · 2026

ОРГАНИЗАЦИОННАЯ МОДЕЛЬ И СОВМЕЩЕНИЕ ФУНКЦИЙ

На дату утверждения настоящего документа функции всех ролей, упомянутых в документе, — Директора (CEO), MLRO (Money Laundering Reporting Officer), Compliance Lead, Risk Committee, ответственного лица за защиту персональных данных, Support Team и Technical Lead — исполняет единолично Директор Компании Кузнецов Роман Игоревич, назначенный Решением единственного участника № 2. Все ссылки в документе на указанные роли и органы следует читать как ссылки на Директора Компании.

При совмещении функций одним лицом применяются следующие правила:

— многоуровневая эскалация (Support → Compliance → MLRO → Risk Committee → CEO) выполняется путём последовательного документирования решения на каждом уровне в журнале эскалаций с указанием оснований; решения без письменного обоснования не допускаются;

— решения, отнесённые к компетенции Risk Committee, оформляются письменным решением Директора с приложением материалов проверки;

— для компенсации отсутствия принципа «четырёх глаз» все решения о принятии High-Risk клиентов, отказах, разблокировке средств, подаче STR/SAR и исключениях из политик фиксируются в журнале, а не реже одного раза в год система AML/CFT проверяется независимым внешним консультантом (аудитором);

— Компания вправе привлечь внешнего MLRO / Compliance-специалиста на условиях аутсорсинга и назначает отдельных лиц на роли MLRO и Compliance Lead по мере роста штата и оборотов, а также по требованию Банков-партнёров, регуляторов или применимого законодательства. Такое назначение оформляется решением Директора и не требует пересмотра документа.

1. Цель и область действия

Настоящая политика устанавливает стандарты противодействия легализации преступных доходов (AML) и финансированию терроризма (CFT), применяемые Free Bird PSP L.L.C-FZ в отношении клиентов, мерчантов и контрагентов.

2. Определения

AML, CFT, KYC, KYB, UBO, PEP, Red Flags, Suspicious Activity, Sanctions Screening, Ongoing Monitoring — используются в значениях, принятых в KYC/KYB Policy Free Bird PSP L.L.C-FZ.

3. Правовая основа

1. Federal Decree-Law No. (10) of 2025 Regarding Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing (ОАЭ) — от 14.10.2025.
2. Cabinet Resolution No. (134) of 2025 — исполнительный регламент к Federal Decree-Law No. 10/2025 от 14.12.2025.
3. Рекомендации FATF (40 Recommendations).
4. Требования банков-партнёров и корреспондентских банков.
5. Санкционные режимы UN, OFAC, EU, UK.
6. Cabinet Decision No. (74) of 2020 concerning the Terrorism Lists Regulation and the Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing (ОАЭ) — правовая основа применяемого Компанией санкционного и террористического скрининга (раздел 12).
7. UAEFIU Regulation No. (1) of 2026 regarding the System Governing the Postponement or Suspension of Suspicious Transactions and the Freezing of Funds — правовая основа процедуры приостановки операций и заморозки средств (раздел 13a).
8. Рекомендации FATF 15 и 16 (виртуальные активы, Travel Rule) — в части расчётов в USDT (раздел 17a).
9. Законодательство Российской Федерации, применимое к Банкам-партнёрам и учитываемое Компанией в части операций по Рублёвым счетам: Федеральные законы № 115-ФЗ «О противодействии легализации (отмыванию) доходов…», № 161-ФЗ «О национальной платёжной системе», № 173-ФЗ «О валютном регулировании и валютном контроле».

4. Ответственность за AML/CFT

Ответственность за функцию AML/CFT распределена в соответствии с governance-структурой Risk Scoring & Acceptance Policy Free Bird PSP L.L.C-FZ:

- MLRO (Money Laundering Reporting Officer) — общая ответственность за AML/CFT, принятие решений по High-Risk кейсам, взаимодействие с регуляторами и подача STR/SAR.
- Compliance Lead — ежедневный мониторинг, подготовка отчётов, первичный анализ красных флагов.
- Risk Committee — коллегиальное рассмотрение спорных случаев.

- CEO — конечная ответственность за систему AML/CFT в целом.

Все сотрудники обязаны соблюдать настоящую политику и немедленно сообщать о подозрительной активности по установленной цепочке эскалации (раздел 13).

На дату утверждения Политики функции MLRO, Compliance Lead, Risk Committee и CEO совмещает Директор Компании Кузнецов Р.И. (см. раздел «Организационная модель и совмещение функций»).

5. Риск-ориентированный подход

Клиенты классифицируются по уровням риска: Low, Medium, High — на основании количественной модели риск-скоринга (0–100 баллов), установленной Risk Scoring & Acceptance Policy. Клиенты категории High Risk (60 баллов и выше) в обязательном порядке проходят усиленную проверку (EDD). Периодический пересмотр профиля клиента: High — раз в 12 месяцев, Medium — раз в 2 года, Low — раз в 3 года, а также внепланово при срабатывании триггеров.

6. Customer Due Diligence (CDD)

Клиентами Компании являются мерчанты — юридические лица. Физические лица проходят идентификацию в качестве UBO (25% и более), директоров, лиц с правом подписи и представителей мерчантов: паспорт / ID, подтверждение адреса (не старше 3 месяцев), скрининг по санкционным спискам, PEP и adverse media.

Для юридических лиц: регистрация, устав, бенефициары, структура владения, сайт, описание деятельности.

Покупатели (плательщики по СБП) не являются клиентами Компании: их идентификацию проводят банки плательщиков. Компания получает сведения о плательщике в объёме, передаваемом Банком-партнёром и оператором СБП (маскированный номер телефона, сокращённое ФИО, банк плательщика, идентификатор операции), и использует их для транзакционного мониторинга (раздел 9).

Политически значимые лица (PEP), члены их семей и близкие лица (RCA): EDD обязателен; устанавливаются источник средств и источник благосостояния (SOF/SOW); решение об установлении или продолжении отношений принимает Директор (senior management approval); профиль пересматривается не реже одного раза в 12 месяцев.

7. Enhanced Due Diligence (EDD)

Применяется при высоких оборотах, подозрительных транзакциях, санкционных связях.

Запрашиваются: договоры, подтверждение источника средств, описание бизнес-процессов, при необходимости — независимый due diligence report.

8. Запрещённые виды деятельности

- обналичивание;
- гемблинг без лицензии;
- мошенничество;
- оружие;

- наркотики;
- даркнет;
- финансовые пирамиды/MLM;
- крипто-миксеры и иные неаудируемые криптосервисы, скрывающие происхождение средств.

Free Bird PSP L.L.C-FZ может отказать в обслуживании мерчанта или клиента без объяснения причин.

9. Мониторинг транзакций

Контроль аномалий по суммам, частоте, юрисдикциям. Подозрительные операции проходят ручную проверку. Все выявленные аномалии фиксируются в журнале.

С учётом модели приёма платежей через СБП (C2B) применяются, как минимум, следующие сценарии мониторинга: концентрация платежей от одних и тех же плательщиков; серии платежей однотипными или круглыми суммами; дробление платежей ниже лимитов; несоответствие суммы платежа среднему чеку и ассортименту мерчанта; всплески оборота относительно заявленного профиля; массовые платежи в ночное время; высокая доля возвратов или попытки возврата на иные реквизиты; платежи от лиц, связанных с самим мерчантом; доля операций без согласия клиента выше 0,05%.

Срабатывания (алерты) рассматриваются не позднее 1 рабочего дня; результат рассмотрения и принятое решение фиксируются в журнале. Пороговые значения сценариев пересматриваются не реже одного раза в 6 месяцев с учётом фактических данных.

10. Red Flags / Триггеры подозрительности

- необычно крупные транзакции;
- высокая частота операций;
- несоответствие транзакций заявленной деятельности;
- использование VPN/прокси;
- множественные IP-адреса за короткий период;
- попытки скрыть источник средств.
- признаки использования счетов «дропов»: множество новых плательщиков, однотипные суммы, платежи одних и тех же лиц в адрес разных мерчантов;
- признаки маскировки P2P-переводов, транзита или вывода капитала под видом оплаты товаров / услуг, в т.ч. в обход валютных ограничений;
- несоответствие оборота мерчанта его сайту, ассортименту и среднему чеку;
- запросы мерчанта на выплату на счета или кошельки третьих лиц, частая смена реквизитов для выплат.

11. Хранение данных

Категория	Срок хранения
KYC/KYB	не менее 5 лет с момента прекращения отношений с клиентом

Транзакции	не менее 5 лет с даты операции
Логи	не менее 12 месяцев
Документы EDD	5–7 лет

12. Санкционный скрининг

Проверка клиентов, мерчантов и UBO по спискам: UN, OFAC SDN, EU, UK HMT, а также по локальному перечню террористических организаций и лиц, формируемому в соответствии с Cabinet Decision No. 74/2020.

Дополнительно применяется «правило 50%» OFAC: если 50% и более капитала контрагента прямо или косвенно принадлежит одному или нескольким лицам из списка SDN, контрагент считается блокированным, даже если сам он в список не включён. При работе с контрагентами и банками-партнёрами, связанными с юрисдикциями, находящимися под секторальными (не только списочными) ограничительными мерами ЕС, США или Великобритании, Compliance Lead дополнительно проверяет применимость таких секторальных ограничений к конкретной операции, помимо стандартного скрининга по спискам.

Поскольку платежи принимаются в рублях от резидентов Российской Федерации через российский Банк-партнёр, Компания дополнительно: проверяет Банки-партнёры и Расчётных партнёров по санкционным спискам UN, ЕС, США и Великобритании до начала и в ходе сотрудничества; оценивает риск вторичных санкций для иностранных финансовых посредников; не допускает операций в интересах лиц под санкциями и операций, направленных на обход санкционных ограничений (в т.ч. оплату товаров двойного назначения).

Адресные финансовые санкции (TFS): при подтверждённом совпадении с Local Terrorist List ОАЭ или Сводным санкционным перечнем СБ ООН Компания незамедлительно (не позднее 24 часов) и без предварительного уведомления клиента замораживает средства и приостанавливает операции, после чего уведомляет Executive Office for Control & Non-Proliferation (EOCN) и надзорный орган через систему goAML в сроки, установленные Cabinet Decision No. 74/2020 и руководствами EOCN. При частичном (возможном) совпадении операции приостанавливаются до его подтверждения или опровержения.

13. Внутренняя отчётность и путь эскалации

Применяется единый для Компании 5-уровневый путь эскалации:

1. Уровень 1 — Support
2. Уровень 2 — Compliance
3. Уровень 3 — MLRO
4. Уровень 4 — Risk Committee
5. Уровень 5 — CEO

Сотрудники обязаны сообщать о подозрительных действиях по данной цепочке. Ведётся внутренний журнал эскалаций.

Подача STR/SAR: решение принимает MLRO; сообщение направляется в UAE FIU через систему goAML незамедлительно после возникновения обоснованного подозрения, независимо от суммы операции и от того, была ли операция проведена. Компания обеспечивает регистрацию в goAML до начала операционной деятельности. Запрещается уведомлять клиента или третьих лиц о направлении или намерении направить STR/SAR (tipping-off).

13a. Приостановка операций и заморозка средств

При выявлении совпадения по санкционным/террористическим спискам (раздел 12), а также при принятии решения о подаче STR/SAR (раздел 13), MLRO вправе принять решение о приостановке (postponement) или полной заморозке (freezing) операции либо средств клиента до выяснения обстоятельств, в порядке, установленном UAEFIU Regulation No. 1/2026.

Решение о приостановке/заморозке, а также о её снятии, фиксируется в журнале эскалаций (раздел 13) с указанием оснований, даты и ответственного лица. Информирование клиента о факте и причинах заморозки осуществляется с учётом правила «tipping-off», если заморозка связана с направлением или намерением направить STR/SAR.

14. Обучение

Обязательное ежегодное обучение всех сотрудников процедурам AML/CFT. Лицо, исполняющее функции MLRO, проходит профильное обучение не реже одного раза в год с подтверждающим документом (сертификатом); материалы и подтверждения обучения хранятся 5 лет.

15. Независимое тестирование программы

Не реже одного раза в 12 месяцев Компания обеспечивает независимое тестирование программы AML/CFT — силами лица или функции, не участвующих в её повседневном исполнении (Compliance Lead, MLRO). При текущем размере и структуре Компании такое тестирование может проводиться внешним консультантом или аудитором, привлекаемым Risk Committee. Результаты тестирования, включая выявленные недостатки и меры по их устранению, оформляются отчётом, рассматриваются Risk Committee и хранятся в порядке, установленном разделом 11 настоящей Политики.

16. Внутренний канал сообщений о нарушениях (Whistleblowing)

Независимо от порядка эскалации по конкретным клиентским кейсам (раздел 13), Компания обеспечивает отдельный конфиденциальный канал, по которому любой сотрудник может сообщить о предполагаемом нарушении требований AML/CFT, включая нарушения со стороны других сотрудников или самой Компании, минуя непосредственного руководителя. Сообщения принимаются по адресу ceo.freebird@gmail.com с прямым доступом Risk Committee и CEO. Компания гарантирует защиту сотрудника, добросовестно сообщившего о нарушении, от преследования и иных неблагоприятных последствий по месту работы.

При совмещении функций одним лицом сообщения о нарушениях могут направляться также непосредственно в UAE FIU или надзорный орган.

17. Риск контрагентов (Third-Party Risk)

Проверка поставщиков KYC-услуг, хостинга и платёжных партнёров на предмет соответствия AML-требованиям и санкционным ограничениям, включая периодический пересмотр статуса таких поставщиков. Если по состоянию на дату актуальной Enterprise Wide Risk Assessment такие сторонние поставщики фактически не привлечены, настоящий раздел действует на перспективу: до заключения договора с любым таким поставщиком в будущем Compliance Lead обязан провести и задокументировать предусмотренную настоящим разделом проверку.

17a. Расчёты в цифровых активах (USDT)

По поручению мерчанта Компания может проводить расчёт по причитающимся ему суммам в цифровой валюте USDT. Компания самостоятельно не осуществляет обмен, хранение (custody) или торговлю цифровыми активами: обмен рублей на USDT и перевод USDT на кошелёк мерчанта выполняет Расчётный партнёр — лицо, имеющее разрешение на оказание услуг с виртуальными активами в своей юрисдикции (например, лицензию VARA (Дубай) или эквивалентную).

Расчёты в USDT относятся к направлениям повышенного риска ОД/ФТ. Применяются следующие обязательные меры:

— due diligence Расчётного партнёра до начала сотрудничества и не реже одного раза в год: лицензия / регистрация, AML/CFT-программа, санкционный скрининг, соблюдение Travel Rule (Рекомендация 16 FATF);

— расчёты в USDT доступны только мерчантам, прошедшим KYB, с уровнем риска не выше Medium; для мерчантов High Risk — только по решению MLRO после EDD;

— принадлежность кошелька мерчанту подтверждается до первой выплаты (тестовая транзакция или подпись сообщения закрытым ключом); адрес вносится в белый список (whitelist), выплаты на иные адреса не проводятся;

— каждый адрес проверяется инструментом блокчейн-аналитики (KYT) до первой выплаты и далее периодически; при выявлении связи адреса с санкционными лицами, миксерами, даркнет-рынками, мошенничеством, похищенными средствами или иными источниками высокого риска выше установленного порога выплата не проводится, вопрос эскалируется на MLRO;

— допускаются только сети TRC-20 и BEP-20; хэш каждой транзакции фиксируется в Платформе и в отчётности мерчанту;

— red flags: частая смена кошельков, запрос выплат на адреса третьих лиц, дробление выплат, адреса с высоким риск-скором, кошельки на биржах без KYC, требование срочной выплаты в обход процедур;

— Компания вправе отказать в расчёте в USDT или приостановить его и провести выплату в рублях при выявлении red flags или санкционных рисков, по требованию Банка-партнёра или государственного органа.

Мерчант самостоятельно отвечает за соблюдение налогового, валютного и иного законодательства своей юрисдикции при получении расчётов в цифровых активах.

18. Отчётность перед регуляторами

Компания предоставляет данные по законному запросу государственных органов, включая UAE FIU (через систему goAML).

19. Пересмотр политики

Политика пересматривается ежегодно либо при изменении законодательства.

Контакты: ceo.freebird@gmail.com