AML (Anti-Money Laundering) – это процесс, который предотвращает использование финансовых инструментов для легализации доходов, полученных незаконным путем. Компании, которые занимаются финансовой деятельностью, должны соблюдать AML-нормативы, включая проведение проверки на соответствие клиента, мониторинг транзакций и уведомление о подозрительных операциях.

CTF (Counter-Terrorism Financing) – это процесс, который предотвращает финансирование террористических организаций. Компании должны проводить проверку на соответствие клиента, мониторинг транзакций и уведомление о подозрительных операциях, чтобы предотвратить финансирование терроризма.

KYC (Know Your Customer) – это процесс, который используется компаниями для проверки личности и финансовых данных клиента. KYC-процедуры включают сбор и анализ документов, установление источника дохода клиента, проведение проверки на соответствие и мониторинг транзакций.

AML/CTF и KYC политика – это правила и процедуры, которые компании используют для борьбы с отмыванием денег и финансированием терроризма. Эти политики помогают идентифицировать клиентов, проверять их личность и финансовые данные, а также отслеживать транзакции, которые могут быть связаны с незаконными действиями.

Цель AML/CTF и KYC политики – предотвращение незаконных действий в финансовой сфере и защита компании от потенциальных рисков. Правильное применение этих политик помогает обеспечить безопасность бизнеса и клиентов, а также поддерживать законность и порядок в финансовой сфере.

AML/CTF (Противодействие отмыванию доходов и финансированию терроризма) и KYC (Знай своего клиента) — это важные инструменты, которые помогают защитить нашу компанию OKANE от рисков незаконной деятельности и обеспечивают безопасность наших клиентов.

AML/CTF Политика включает в себя следующие меры:

1. Идентификация клиентов и проверка их личности. Для этого OKANE может использовать различные методы, такие как запрос документов, проведение онлайн-проверок и т.д;
2. Мониторинг транзакций клиентов для обнаружения подозрительных операций. Если обнаруживаются подозрительные операции, OKANE в праве приостановить транзакцию клиента;
3. Обучение персонала OKANE правилам AML/CTF и создание процедур для обработки подозрительных транзакций.

KYC Политика включает в себя следующие меры:

1. Сбор информации о клиентах, включая их личные данные, источник дохода и т.д;
2. Проверка и подтверждение данных клиента через различные источники;
3. Оценка рисков, связанных с клиентом, и принятие соответствующих мер для минимизации этих рисков;
4. Обновление информации о клиентах в соответствии с изменениями их личных данных.

Для определения таких транзакций обменный сервис OKANE использует специализированные сервисы проверок транзакций.

1. В случае, если AML риск по транзакции превышает значение 70% будет заморожена, но в некоторых случаях заморозка средств может произойти при оценке меньше, чем 70%, и такие транзакции рассматриваются в индивидуальном порядке;
2. Транзакции с под санкционных сервисов будут заморожены, несмотря на уровень риска операции;
3. Если на транзакции стоит отметка victim-report (это значит что данная транзакция имеет связь с официальным уголовным делом) — она также будет заблокирована;

К каждому случаю AML мы подходим индивидуально и опираясь на много факторов, дата совершения транзакции, процентное соотношение средств на адресе, не "размывали" ли другими транзакциями риск-скор и т.д.

В случае, если пользователь отправляет актив, имеющий маркировку «санкции» или «миксер», его средства могут быть заморожены регулятором на неопределенный срок. Обменный пункт не несет ответственности за возврат средств с указанными выше опасными источниками!

В случае нарушения правил AML/CTF и KYC Политики сервис оставляет за собой право:

1. Приостановить транзакцию;
2. Запросить у пользователя фото или видео с документом, подтверждающим личность пользователя (Селфи);
3. Запросить у пользователя Скрин из ЛК кошелька вывода криптовалюты;
4. Заблокировать аккаунт и любые операции, связанные с пользователем, передать в контролирующие финансовую деятельность и/или правоохранительные органы по месту регистрации Сервиса;
5. Удерживать средства пользователя до полного расследования инцидента;
6. Осуществлять возврат цифровых активов только на реквизиты, с которых перевод был осуществлен или перейти на другие реквизиты, после полной проверки

службой безопасности Сервиса, если удалось проверить легальное происхождение средств пользователя;

7. Запрашивать у пользователя иные материалы и документы касающиеся обмена.
8. В случае если пользователь не предоставляет запрошенную информацию и не отвечает на запросы сервиса в течении 3 календарных месяцев, удержанные средства не возвращаются.