УТВЕРЖДАЮ
Председатель Правления
РНКО «Платежный Центр» (ООО)

Мац Г.М.

27 апреля 2020 года

ПОЛИТИКА
ПЛАТЕЖНОЙ СИСТЕМЫ «ЗОЛОТАЯ КОРОНА»
В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

ОГЛАВЛЕНИЕ

1. ИСПОЛЬЗУЕМАЯ ТЕРМИНОЛОГИЯ

Термины и сокращения, используемые в настоящей **ПОЛИТИКЕ**, определяются **СЛОВАРЕМ ТЕРМИНОВ**, а также **ПРАВИЛАМИ СИСТЕМЫ, ПРАВИЛАМИ СЕРВИСА** и настоящей **ПОЛИТИКОЙ**.

Направление – совокупность **СУБЪЕКТОВ**, объединенных по территориальному признаку (страна, город);

Ответственный сотрудник – специальное должностное лицо, ответственное за соблюдение у **СУБЪЕКТА** норм законодательства в области ПОД/ФТ;

ПОД/ФТ – противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

Сотрудник **СИСТЕМЫ** – сотрудник **СИСТЕМЫ,** уполномоченный взаимодействовать с **СУБЪЕКТАМИ** в рамках реализации данной Политики;

Сомнительные операции - это операции, осуществляемые **КЛИЕНТАМИ**, имеющие необычный характер и признаки отсутствия явного экономического смысла и очевидных законных целей.

Список – «Список сомнительных клиентов» – список лиц, операции которых не проводятся в **СИСТЕМЕ**;

Уполномоченный орган – орган, осуществляющий функции национальной службы финансовой разведки в соответствии с законодательством той или иной страны, в адрес которого **СУБЪЕКТЫ** организации (в частности, **УЧАСТНИКИ**) обязаны направлять информацию о сомнительных операциях;

Черные списки – правительственные, международные перечни организаций (в том числе юридических лиц) и/или физических лиц, в отношении которых имеются сведения об их причастности к отмыванию доходов, полученных преступным путем, финансированию экстремистской деятельности и терроризма, финансированию оружия массового уничтожения.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая **ПОЛИТИКА** является **ЛОКАЛЬНЫМ ДОКУМЕНТОМ**, определяющим общие принципы и подходы **СИСТЕМЫ,** основные направления и мероприятия, реализуемые в рамках **СИСТЕМЫ** и **СЕРВИСА** в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма,

Настоящая **ПОЛИТИКА** обязательна для исполнения всеми **СУБЪЕКТАМИ** и публикуется на **САЙТЕ**.

ОПЕРАТОР вправе в одностороннем внесудебном порядке вносить изменения в настоящую **ПОЛИТИКУ** путем размещения новой редакции **ПОЛИТИКИ** на **САЙТЕ** не менее чем за 15 (Пятнадцать) календарных дней до вступления их в силу.

Нормы **ПОЛИТИКИ** могут быть применены на территории любой страны, поскольку она не содержит требований «противолегализационного» законодательства отдельных государств, а определяет общие принципы и подходы **СИСТЕМЫ** в целях ПОД/ФТ.

Данный документ разработан с целью предотвращения использования **СИСТЕМЫ** и ее **УЧАСТНИКОВ/ПАРТНЕРОВ** в процессе легализации незаконно полученных средств, а также снижения рисков их вовлечения в незаконный оборот наличных денежных средств.

СИСТЕМА не поддерживает деловых отношений с **УЧАСТНИКАМИ/ПАРТНЕРАМИ**, сознательно идущими на нарушение законодательства в области ПОД/ФТ. Необходимым условием для возможности работы **УЧАСТНИКА/ПАРТНЕРА** в рамках **СИСТЕМЫ/СЕРВИСА** является наличие разработанных **УЧАСТНИКОМ/ ПАРТНЕРОМ** процедур и проведение мероприятий в целях ПОД/ФТ.

Процедуры, содержащиеся в **ПОЛИТИКЕ**, призваны наладить результативное взаимодействие **СИСТЕМЫ/СЕРВИСА** с **УЧАСТНИКАМИ/ПАРТНЕРАМИ** с целью обеспечения единого подхода к выявлению операций, имеющих признаки сомнительности. С этой целью **ОПЕРАТОРОМ** проводится сбор информации о критериях, применяемых **УЧАСТНИКОМ/ПАРТНЕРОМ** при выявлении сомнительных операций. На основании полученных критериев **ОПЕРАТОРОМ** проводится мониторинг операций, с последующим информированием **УЧАСТНИКОВ/ПЕРАТНЕРОВ** об операциях **КЛИЕНТОВ**, подпадающих под указанные критерии.

УЧАСТНИКИ/ПАРТНЕРЫ обязаны соблюдать нормы законодательства в области противодействия легализации доходов, полученных преступным путем, и финансированию терроризма страны, резидентом которой они являются, в том числе обязаны обеспечивать выполнение действующих требований и рекомендаций Международных стандартов по противодействию отмыванию доходов, финансированию терроризма и распространению оружия массового уничтожения (FATF, 2012), а также выполнять требования настоящей **ПОЛИТИКИ**. Невыполнение указанных требований может повлечь за собой прекращение **ОПЕРАТОРОМ** сотрудничества с таким **УЧАСТНИКОМ/ПАРТНЕРОМ**.

Законы большинства стран рассматривают отмывание денег как тяжкое

преступление, предусматривая наказание в виде штрафов и лишения свободы на достаточно длительные сроки. Также, несоблюдение законодательства в области противодействия легализации доходов, полученных преступным путем, может повлечь за собой серьезные последствия для **УЧАСТНИКА/ПАРТНЕРА** в виде применения мер воздействия со стороны надзорных органов.

ПОЛИТИКА призвана оказать методическую помощь **УЧАСТНИКАМ/ПАРТНЕРАМ** в текущей работе. Использование разработанных рекомендаций в практической деятельности каждым работником **УЧАСТНИКА/ПАРТНЕРА** является обязательным. **УЧАСТНИКИ/ПАРТНЕРЫ** могут использовать материалы, содержащиеся в настоящей **ПОЛИТИКЕ**, при проведении инструктажей своих работников.

Помимо требований законодательства в области ПОД/ФТ и требований, изложенных в **ПОЛИТИКЕ**, **УЧАСТНИКИ/ПАРТНЕРЫ** обязаны соблюдать нормативные акты страны, резидентом которой они являются, регулирующие операции перевода денежных средств без открытия счета. **ОПЕРАТОР**, в свою очередь, обязуется оказывать всестороннюю методическую и практическую помощь **УЧАСТНИКАМ/ПАРТНЕРАМ** в реализации разработанных ими мероприятий. Так, **ОПЕРАТОР** курирует **УЧАСТНИКОВ/ПАРТНЕРОВ** на постоянной основе, в частности, доводит до них информацию о сомнительных операциях, проводимых их **КЛИЕНТАМИ**.

СУБЪЕКТЫ обязаны предоставлять **ОПЕРАТОРУ** по его запросу любую информацию, необходимую для подтверждения **СУБЪЕКТОМ** своих обязательств по осуществлению в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. **УЧАСТНИК**, являющийся иностранным поставщиком платежных услуг, предоставляющий **КЛИЕНТАМ** электронные средства платежа, прием которых осуществляется на территории Российской Федерации, обязан по запросу **ОПЕРАТОРА** в срок не позднее 3 (Трех) рабочих дней со дня получения такого запроса, предоставить сведения о **КЛИЕНТАХ**, полученные таким **УЧАСТНИКОМ** при проведении идентификации в соответствии с требованиями страны юрисдикции **УЧАСТНИКА**.

Используемые **СУБЪЕКТАМИ ПАК,** а также третьи лица, привлекаемые **СУБЪЕКТАМИ** к осуществлению **ПЕРЕВОДОВ**, должны соответствовать требованиям, предусмотренным **ПРАВИЛАМИ, ПРАВИЛАМИ СЕРВИСА,** настоящей **ПОЛИТИКИ**.

СУБЪЕКТЫ обязаны обеспечить хранение всех документов, относящихся к **ПЛАТЕЛЬЩИКАМ** и **ПЕРЕВОДАМ**, выполненных на бумажных носителях, в течение пяти лет после совершения **ПЕРЕВОДА** и обеспечить передачу таких документов в уполномоченные государственные органы, осуществляющие меры по противодействию, по надлежащему запросу последних (Рекомендации 11 и 16 FATF).

За неисполнение/ненадлежащее соблюдения настоящей **ПОЛИТИКИ СУБЪЕКТЫ** несут ответственность в соответствии законодательством инкорпорации **СУБЪЕКТОВ**.

3. ОТМЫВАНИЕ ДЕНЕГ. ПРИНЦИП ДЕЙСТВИЯ

Общий принцип действия при отмывании денег отсутствует. Однако типичные примеры отмывания денег исторически складываются из трех этапов:

1. **Размещение:** В первой фазе незаконно приобретенные имущественные ценности размещаются в легальные финансовые инструменты, чтобы обезличить доходы и сделать их мобильными.
2. **Разбивка:** Во второй фазе криминальные и легально приобретенные имущественные ценности смешиваются, при этом зачастую незаконные доходы уходят за пределы страны, или же их происхождение стирается иным образом.
3. **Интеграция:** В третьей фазе «отмытые» имущественные ценности снова вводятся в легальную экономику путем инвестирования или приобретения недвижимости, автомобилей, предметов роскоши.

Не редки случаи, когда доходы, прошедшие все этапы отмывания, в дальнейшем используются в целях финансирования преступной либо террористической деятельности.

Современные меры по борьбе с отмыванием денег применяются в основном в первой фазе (размещение). В значительно меньшей степени во второй фазе (разбивка) и лишь совсем в редких случаях в третьей фазе (интеграция).

Так, незаконные прибыли от торговли наркотиками или оружием сначала появляются в виде наличных денег и отмываются в виде закупки и перепродажи товаров. Имущественные ценности, которые перемещаются исключительно в криминальном теневом секторе экономики трудно обнаружить. Но когда имущественные ценности помещаются в легальный сектор экономики, например, осуществляется перевод денежных средств или внесение наличных денег на банковский счет, появляется возможность обнаружить нелегальные денежные средства.

Таким образом, понятие «отмывание денег» подразумевает деятельность по приданию правомерного вида владению, пользованию или распоряжению денежными средствами, полученными в результате совершения преступления.

Данное определение подразумевает под собой широкий спектр деятельности, который не ограничивается каким либо типом операций, будь то безналичные операции, либо операции с наличной валютой. В процесс отмывания денег может быть вовлечен любой финансовый инструмент, не исключая и денежные переводы.

Очевидно, что общепринятое определение или объяснение отдельных способов отмывания денег бессмысленно, поскольку техника отмывания развивается параллельно с усовершенствованием предупредительных мер. Сложность создания эффективных предупредительных мер заключается также в том, что системы предупреждения можно лишь приспособить к уже имеющимся направлениям в отмывании.

В целях предотвращения отмывания денег **УЧАСТНИКУ/ПАРТНЕРУ** необходимо четко исполнять требования законодательства в области ПОД/ФТ страны, резидентом которой является **УЧАСТНИКИ/ПАРТНЕРЫ**.

Все работники **УЧАСТНИКА/ПАРТНЕРА**, участвующие в осуществлении **ПЕРЕВОДОВ**, как принимающие **ПЕРЕВОДЫ**, так и выдающие их, должны знать о мерах ответственности, которые могут быть применены как к должностным лицам **УЧАСТНИКА/ПАРТНЕРА**, так и к самому **УЧАСТНИКУ/ПАРТНЕРУ** в случае неисполнения либо ненадлежащего исполнения норм законодательства в области ПОД/ФТ.

4. РИСКИ, СВЯЗАННЫЕ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ И ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА

При реализации норм законодательства в рамках осуществления своей профессиональной деятельности **УЧАСТНИКИ/ПАРТНЕРЫ** могут столкнуться со следующими видами рисков:

- Риск потери деловой репутации;
- Правовой риск;
- Риск вовлечения сотрудников в противоправную деятельность;
- Риск применения мер воздействия.

Указанный перечень не является исчерпывающим. В зависимости от специфики операций, проводимых **УЧАСТНИКОМ/ПАРТНЕРОМ** и его **КЛИЕНТАМИ**, **УЧАСТНИК/ПАРТНЕР** самостоятельно оценивает возникающие риски и принимает меры к их снижению.

4.1. РИСК ПОТЕРИ ДЕЛОВОЙ РЕПУТАЦИИ (РЕПУТАЦИОННЫЙ РИСК)

Риск потери деловой репутации может быть вызван неспособностью **УЧАСТНИКА/ПАРТНЕРА** эффективно противодействовать противоправной деятельности, осуществляемой недобросовестными **КЛИЕНТАМИ**, в частности – деятельности по легализации денежных средств и финансированию терроризма.

Недостатки в организации системы внутреннего контроля в целях противодействия легализации денежных средств и финансированию терроризма могут стать причиной возникновения репутационного риска.

Указанный риск также может быть вызван таким негативным фактором, как недостатки в кадровой политике, обучении работников.

4.2. ПРАВОВОЙ РИСК

Повышение уровня правового риска может быть обусловлено таким фактором, как несоблюдение **УЧАСТНИКОМ/ПАРТНЕРОМ** законодательства страны, резидентом которой является **УЧАСТНИК/ПАРТНЕР**, в области ПОД/ФТ, в том числе по идентификации **КЛИЕНТОВ**.

Неэффективная организация правовой работы, а как следствие несоответствие внутренних документов **УЧАСТНИКА/ПАРТНЕРА** законодательству в области ПОД/ФТ также является причиной возникновения указанного вида риска.

4.3. РИСК ВОВЛЕЧЕНИЯ СОТРУДНИКОВ В ПРОТИВОПРАВНУЮ ДЕЯТЕЛЬНОСТЬ (КАДРОВЫЙ РИСК)

Возможное несоблюдение работниками **УЧАСТНИКА/ПАРТНЕРА** принципов профессиональной этики при обслуживании **КЛИЕНТОВ**, несоблюдение правил установленных настоящей **ПОЛИТИКОЙ** может повлечь за собой как репутационные, так и правовые риски.

Недостатки кадровой политики, такие как несоблюдение квалификационных требований к работникам, а также требований по подготовке и обучению кадров в соответствии с характером их профессиональной деятельности, являются немаловажным фактором в формировании кадрового риска и могут стать причиной вовлечения **УЧАСТНИКА/ПАРТНЕРА** в незаконный оборот наличных денежных средств.

4.4. РИСК, СВЯЗАННЫЙ С ОРГАНАМИ НАДЗОРА (РИСК ПРИМЕНЕНИЯ МЕР ВОЗДЕЙСТВИЯ)

Вовлечение **УЧАСТНИКА/ПАРТНЕРА** в нелегальные схемы расчетов может послужить причиной проявления внимания со стороны правоохранительных органов, а возможные судебные разбирательства и связанное с этим обсуждение в СМИ повлечет за собой помимо риска применения штрафных санкций, также и репутационный риск.

Надзорными органами по результату проводимых проверок также могут быть применены меры воздействия к **УЧАСТНИКУ/ПАРТНЕРУ**.

В Российской Федерации предусмотрены такие меры воздействия к кредитным организациям как наложение штрафов, приостановление проведения определенного вида операций, запрет на открытие счетов, приостановление деятельности организации, а также отзыв лицензии.

5. УПРАВЛЕНИЕ РИСКАМИ, СВЯЗАННЫМИ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ И ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА

УЧАСТНИКИ/ПАРТНЕРЫ как субъекты исполнения законодательства в области ПОД/ФТ заинтересованы в сохранении стабильности и высокой профессиональной репутации. Управление рисками при исполнении законодательства в области ПОД/ФТ осуществляется посредством налаженной системы внутреннего контроля. Контроль за организацией у **УЧАСТНИКА/ПАРТНЕРА** противодействия легализации доходов возлагается на руководителя **УЧАСТНИКА/ПАРТНЕРА**.

У **УЧАСТНИКА/ПАРТНЕРА** должны проводиться мероприятия в рамках исполнения противолегализационного контроля, а именно:

- Назначено должностное лицо, ответственное за соблюдение у **УЧАСТНИКА/ПАРТНЕРА** норм законодательства в целях ПОД/ФТ (Ответственный сотрудник).
- Разработаны внутренние документы, содержащие процедуры и мероприятия по ПОД/ФТ.
- Обеспечение участия всех работников **УЧАСТНИКА/ПАРТНЕРА** независимо от занимаемой должности в рамках их компетенции в выявлении сомнительных операций.
- Соблюдение принципа «Знай своего клиента» «Know Your Client»: проведение на основании официальных документов идентификации **КЛИЕНТА**.
- Проведение мероприятий по выявлению операций, имеющих признаки сомнительности, и представление информации о них национальной службе финансовой разведки.
- Соблюдение всеми работниками **УЧАСТНИКА/ПАРТНЕРА** требования о конфиденциальности информации и запрет на информирование **КЛИЕНТА** о мероприятиях, проводимых у **УЧАСТНИКА/ПАРТНЕРА** в целях ПОД/ФТ.
- Проведение на регулярной основе обучения всех работников, а также мероприятий по проверке знаний.
- Применение мер воздействия к работникам за ненадлежащее исполнение норм законодательства по ПОД/ФТ.
- Постоянный мониторинг системы противолегализационного контроля **УЧАСТНИКА/ПАРТНЕРА**, как специальным внутренним подразделением **УЧАСТНИКА/ПАРТНЕРА**, так и независимыми сторонними организациями.

6. МЕРЫ, ПРЕДПРИНИМАЕМЫЕ УЧАСТНИКОМ/ПАРТНЕРОМ В ЦЕЛЯХ ПОД/ФТ

ОПЕРАТОР определяет единые стандарты в подходе **УЧАСТНИКОВ/ПАРТНЕРОВ** к вопросу выявления сомнительных операций, тогда как **УЧАСТНИКИ/ПАРТНЕРЫ**, исходя из практики осуществления денежных **ПЕРЕВОДОВ** и с учетом требований национального законодательства в области ПОД/ФТ, формируют свои критерии и признаки сомнительных операций. При разработке **УЧАСТНИКОМ/ПАРТНЕРОМ** внутреннего документа, содержащего процедуры исполнения законодательства в области ПОД/ФТ, **УЧАСТНИК/ПАРТНЕР** выстраивает система внутреннего контроля, и разрабатывает мероприятия по управлению рисками.

УЧАСТНИКИ/ПАРТНЕРЫ, имеющие филиальную сеть (внутренние структурные подразделения), обеспечивают контроль за выполнением норм, изложенных во внутренних документах **УЧАСТНИКА/ПАРТНЕРА** и в настоящей **ПОЛИТИКЕ**, во всех филиалах (внутренних структурных подразделениях).

УЧАСТНИК/ПАРТНЕР назначает должностных лиц, ответственных за соблюдение норм законодательства в целях ПОД/ФТ – Ответственный сотрудник. При назначении Ответственного сотрудника, к нему предъявляется ряд требований в части образования, квалификации, опыта работы.

Под руководством Ответственного сотрудника может быть создано подразделение, в обязанности которого входит реализация мероприятий по исполнению требований законодательства по ПОД/ФТ. Сотрудники подразделения по противодействию должны быть наделены достаточно широким спектром полномочий, позволяющим им исполнять свои должностные обязанности.

Принципиальным требованием к деятельности Ответственного сотрудника является его независимость от других подразделений и прямое подчинение руководству **УЧАСТНИКА/ПАРТНЕРА**.

УЧАСТНИК/ПАРТНЕР обязан разработать процедуры, обеспечивающие исполнение национального законодательства в целях ПОД/ФТ. Указанные процедуры и документы, разработанные в целях ПОД/ФТ на регулярной основе должны подвергаться анализу с внесением изменений согласно действующему законодательству.

Наличие разработанных **УЧАСТНИКОМ/ПАРТНЕРОМ** процедур и проведение мероприятий в целях ПОД/ФТ является необходимым условием для возможности работы **УЧАСТНИКА/ПАРТНЕРА** в рамках **СИСТЕМЫ/СЕРВИСА**.

Помимо общих принципов и подходов, реализуемых **УЧАСТНИКОМ/ПАРТНЕРОМ**, указанные документы должны содержать критерии и признаки сомнительности операций, разработанные в зависимости от специфики деятельности **УЧАСТНИКА/ПАРТНЕРА** и его **КЛИЕНТОВ**.

Немаловажным является разработка инструктивного материала для каждого подразделения **УЧАСТНИКА/ПАРТНЕРА** в зависимости от выполняемых работниками функций.

Обеспечение выполнения требования о вовлечении всех работников **УЧАСТНИКА/ПАРТНЕРА** в осуществление мероприятий по ПОД/ФТ обеспечивается включением указанных требований в должностные обязанности, проведением обучающих мероприятий.

Обучение работников должно осуществляться на постоянной основе. В рамках обучающих мероприятий должны освещаться вопросы, касающиеся клиентской базы **УЧАСТНИКА/ПАРТНЕРА**, проводимых ими операций, с освещением типологий проведения сомнительных операций.

Обязательным является ознакомление работников в рамках обучающих мероприятий с требованием о конфиденциальности информации. работникам запрещается консультировать **КЛИЕНТОВ** о возможностях уклонения от процедур контроля в рамках ПОД/ФТ.

Также в рамках обучающих мероприятий работники должны знакомиться с мерами воздействия, которые могут быть применены к должностным лицам либо к **УЧАСТНИКУ/ПАРТНЕРУ** за неисполнение законодательства в области ПОД/ФТ.

На регулярной основе необходимо проводить проверку знаний работников. По результатам проводимых проверок принимается решение о соответствии работников квалификационным требованиям, предъявляемым к занимаемым ими должностям.

Во внутренних документах **УЧАСТНИК/ПАРТНЕР** определяет программу идентификации **КЛИЕНТОВ**, включающую процедуры сбора и фиксирования информации о **КЛИЕНТЕ** в целях соблюдения принципа «Знай своего клиента».

Требования по проведению идентификации **КЛИЕНТОВ** могут отличаться в зависимости от требований законодательства страны, резидентом которой является **УЧАСТНИК/ПАРТНЕР**.

Объемы информации, устанавливаемой в целях идентификации **КЛИЕНТОВ**, определяются **УЧАСТНИКОМ/ПАРТНЕРОМ** дифференцированно в зависимости от характера и особенностей осуществляемых банковских операций, от предполагаемой продолжительности договорных отношений с **КЛИЕНТОМ**, предполагаемого объема операций **КЛИЕНТА**.

Требования по обязательному проведению идентификации **КЛИЕНТА** в полном объеме возникают у **УЧАСТНИКА/ПАРТНЕРА** в случае, когда операции, проводимые **КЛИЕНТОВ**, вызывают у **УЧАСТНИКА/ПАРТНЕРА** подозрения в том, что они проводятся в целях легализации денежных средств и финансирования терроризма.

В случае отнесения операций **КЛИЕНТОВ** к сомнительным (на основании

критериев зафиксированных во внутренних документах **УЧАСТНИКА/ПАРТНЕРА**) согласно законодательству многих стран у **УЧАСТНИКА/ПАРТНЕРА** возникает обязанность по предоставление информации о данной операции в адрес национальной службы финансовой разведки.

Порядок предоставления информации о таких операциях также фиксируется во внутренних документах **УЧАСТНИКА/ПАРТНЕРА**.

В случае возникновения подозрений, что операция с использованием электронного средства платежа, предоставленного **КЛИЕНТУ УЧАСТНИКОМ**, являющимся иностранным поставщиком платежных услуг, осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, **ОПЕРАТОР** обязан запрашивать у такого **УЧАСТНИКА** сведения, полученных при идентификации **КЛИЕНТА**, согласно условиям и положениям настоящей **ПОЛИТИКИ**.

7. СОБЛЮДЕНИЕ ПРИНЦИПА «ЗНАЙ СВОЕГО КЛИЕНТА» «KNOW YOUR CLIENT»

Реализация принципа «Знай своего клиента» - обязательство, принимаемое на себя **УЧАСТНИКОМ/ПАРТНЕРОМ** согласно требованиям законодательства, нормативных документов, а также настоящей **ПОЛИТИКИ**.

Порядок идентификации **КЛИЕНТОВ** и объемы устанавливаемых данных определяются в договорах и соглашениях между **УЧАСТНИКОМ/ПАРТНЕРОМ** и его **КЛИЕНТАМИ**, а также внутренними правилами, инструкциями и иными документами, принятыми **УЧАСТНИКОМ/ПАРТНЕРОМ**.

При обращении **КЛИЕНТА** работник **УЧАСТНИКА/ПАРТНЕРА** выясняет, действует ли **КЛИЕНТ** от своего имени либо по поручению на основании доверенности.

Работник проводит идентификацию **КЛИЕНТА**, фиксирует сведения, необходимые для идентификации. Идентификация физических лиц должна проводиться на основании документа, удостоверяющего личность. При проведении процедуры идентификации **КЛИЕНТА** работник **УЧАСТНИКА/ПАРТНЕРА** обращает внимание на то, чтобы все документы были действительными на дату их предъявления.

Одновременно при фиксировании сведений предусмотрена процедура проверки участников проводимой операции на упоминание о них в правительственных перечнях.

Также в ряде стран предусмотрена обязанность **УЧАСТНИКОВ/ПАРТНЕРОВ** при принятии на обслуживание **КЛИЕНТОВ** принимать меры к выявлению среди них публичных должностных лиц «Politically Exposed Persons».

В зависимости от требований национального законодательства объем данных, необходимых для проведения идентификации **КЛИЕНТА**, может отличаться.

УЧАСТНИКУ/ПАРТНЕРУ для идентификации **КЛИЕНТА** необходимо установить следующие данные:

- фамилия, имя, отчество (при наличии);
- гражданство;
- дата рождения;
- тип документа, удостоверяющего личность;
- серия документа, удостоверяющего личность;
- номер документа, удостоверяющего личность;
- дата выдачи документа, удостоверяющего личность;
- наименование органа, выдавшего документ, удостоверяющий личность;
- место жительства / регистрации.

Законодательством ряда стран предусмотрено проведение операций до определенных суммовых порогов при отсутствии идентификации **КЛИЕНТОВ**. В таких случаях **СИСТЕМА/СЕРВИС** рекомендует проводить идентификацию **КЛИЕНТА** в стандартных объемах.

При непосредственном обслуживании **КЛИЕНТА** в случае, если у работника **УЧАСТНИКА/ПАРТНЕРА** возникают подозрения, что операция **КЛИЕНТА** осуществляется в целях легализации денег, финансирования терроризма или имеет иные признаки сомнительности, работником принимаются меры к проведению более полной идентификации **КЛИЕНТА**.

В случае отказа **КЛИЕНТА** от проведения идентификации в полном объеме, а также отказа **КЛИЕНТА** от предоставления работнику **УЧАСТНИКА/ПАРТНЕРА** объяснений или документов, запрашиваемых в целях исполнения законодательства в области ПОД/ФТ, данному **КЛИЕНТУ** отказывается в обслуживании.

7.1. ОСУЩЕСТВЛЕНИЕ ОПЕРАЦИЙ ЛИЦАМИ, ДЕЙСТВУЮЩИМИ НА ОСНОВАНИИ ДОВЕРЕННОСТИ

В случае если от имени **КЛИЕНТА** к **УЧАСТНИКУ/ПАРТНЕРУ** обратился его представитель, действующий на основании доверенности, работник **УЧАСТНИКА/ПАРТНЕРА** отказывает в осуществлении операции.

Указанное требование действует как при осуществлении операций по приему или выдаче денежного **ПЕРЕВОДА**, так и при его отзыве.

7.2. ПРОВЕРКА КЛИЕНТОВ НА УПОМИНАНИЕ В ПРАВИТЕЛЬСТВЕННЫХ ПЕРЕЧНЯХ

Законодательство многих стран объединено требованием об обязательном информировании органа национальной финансовой разведки об операциях лиц, причастных к террористической деятельности, финансированию распространения оружия массового уничтожения.

Также требованием законодательства ряда стран, а также обязательствами, определенными в резолюции Совета безопасности ООН о предотвращении и противодействии терроризму, в частности Резолюций 1267, 1373 и следующих, связанных с ними резолюций ООО (Рекомендация 16 FATF) является приостановление (прекращение) операций, связанных с финансированием терроризма.

В этих целях правительством доводятся до финансовых институтов перечни с указанием в них лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, финансированию распространения оружия массового уничтожения.

ОПЕРАТОР с помощью программно-аппаратного комплекса **СИСТЕМЫ** обеспечивает возможность осуществления **УЧАСТНИКОМ/ПАРТНЕРОМ** сличения данных **КЛИЕНТА** с данными, содержащимися в Черных списках, полученных **ОПЕРАТОРОМ** на законных основаниях, а также в порядке, определенном законодательством Российской Федерации.

При проведении процедуры идентификации **КЛИЕНТА** проводится сличение данных **КЛИЕНТА** с данными, содержащимися в Черных списках. Как правило, при

выявлении **КЛИЕНТА**, данные которого совпали с данными, имеющимися в Черных списках, необходимо провести более полную идентификацию **КЛИЕНТА** с целью установления идентичности личности **КЛИЕНТА**, обратившегося к **УЧАСТНИКУ/ПАРТНЕРУ**, и указанной в перечне.

В случае выявления операций **КЛИЕНТА**, информация о котором содержится в Черных списках, **УЧАСТНИКУ/ПАРТНЕРУ** необходимо провести мероприятия согласно внутренним документам, также проинформировать органы национальной финансовой разведки о данной операции.

К примеру, в Российской Федерации операции лиц, включенных в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности и терроризму, подлежат приостановлению на 5 рабочих дня с незамедлительным информированием Федеральной службы по финансовому мониторингу об указанной операции. В случае, если **УЧАСТНИКОМ/ПАРТНЕРОМ** в течение срока приостановления не будет получено указания о дополнительном приостановлении операции, такая операция может быть проведена.

7.3. ВЫЯВЛЕНИЕ ПУБЛИЧНЫХ ДОЛЖНОСТНЫХ ЛИЦ «POLITICALLY EXPOSED PERSONS»

В целях управления рисками законодательством ряда стран предусмотрена обязанность **УЧАСТНИКОВ/ПАРТНЕРОВ** по установлению среди лиц, принимаемых на обслуживание, публичных должностных лиц и их родственников. Соответствующие процедуры (по выявлению, принятию на обслуживание и т. д.) должны содержаться во внутренних документах **УЧАСТНИКА/ПАРТНЕРА**.

Решение о принятии на обслуживание указанных лиц принимается высшим руководством **УЧАСТНИКА/ПАРТНЕРА**. В случае принятия решения об обслуживании такого **КЛИЕНТА УЧАСТНИКОМ/ПАРТНЕРОМ** должны приниматься меры по выявлению источников происхождения его денежных средств.

Также в обязанности **УЧАСТНИКА/ПАРТНЕРА**, принявшего на обслуживание указанное лицо, входит проявление повышенного внимания к операциям с денежными средствами такого **КЛИЕНТА**.

7.4. ОТДЕЛЬНЫЕ СЛУЧАИ, КОГДА ТРЕБУЕТСЯ ПРОВЕСТИ ИДЕНТИФИКАЦИЮ КЛИЕНТА В ПОЛНОМ ОБЪЕМЕ

Внутренние документы **УЧАСТНИКА/ПАРТНЕРА** должны содержать процедуры, определяющие порядок проведения идентификации **КЛИЕНТОВ**. В частности, в указанных документах должны быть перечислены данные, которые необходимо зафиксировать при осуществлении **ПЕРЕВОДА** (Рекомендация 16 FATF). Также в указанных документах должны быть перечислены случаи, когда работнику **УЧАСТНИКА/ПАРТНЕРА** необходимо установить дополнительные данные о физическом лице, совершающем операцию.

Так, проведение идентификации в более полном объеме может потребоваться в следующих случаях:

- При полном или частичном совпадении фамилии, имени, отчества с данными, содержащимися в Черных списках, работнику **УЧАСТНИКА/ПАРТНЕРА** необходимо установить и зафиксировать более подробные данные о физическом лице, на основании которых он может сделать однозначный вывод о совпадении личности **КЛИЕНТА** с данными из перечня.
- В случае если согласно национальному законодательству, по каким либо критериям (сумма операции, состав участников и т. д.) информация об операции должна быть представлена в органы финансовой разведки то необходимо провести идентификацию **КЛИЕНТА** в полном объеме для представления указанной информации о **КЛИЕНТЕ** в соответствующие органы.
- Если при проведении операции **КЛИЕНТА** у работника **УЧАСТНИКА/ПАРТНЕРА** возникают подозрения, что данные операции осуществляются в целях легализации денег или финансирования терроризма, работник **УЧАСТНИКА/ПАРТНЕРА** может провести более подробную идентификацию **КЛИЕНТА**. Подробнее о критериях выявления сомнительных операций указано в п. 8 настоящей Политики.
- В случае если операции **КЛИЕНТА** были расценены Ответственным сотрудником **УЧАСТНИКА/ПАРТНЕРА** как подозрительные, то для представления информации о них в органы национальной финансовой разведки необходимо зафиксировать полный объем данных о **КЛИЕНТЕ**.
- При квалификации операций **КЛИЕНТА** как сомнительных, Ответственный сотрудник **УЧАСТНИКА/ПАРТНЕРА** инициирует решение о внесении указанного **КЛИЕНТА** в «Список сомнительных клиентов». В таком случае необходимо провести полную идентификацию **КЛИЕНТА** с целью направления в адрес **ОПЕРАТОРА** информации о **КЛИЕНТЕ** и проводимых им операциях.

Также при проведении операций **КЛИЕНТА**, которые, по мнению работника **УЧАСТНИКА/ПАРТНЕРА**, имеют признаки сомнительности, работником **УЧАСТНИКА/ПАРТНЕРА** могут быть запрошены дополнительные данные и документы, необходимые для классификации операции.

8. РЕКОМЕНДАЦИИ УЧАСТНИКАМ/ПАРТНЕРАМ

В целях создания эффективно функционирующей системы выявления сомнительных операций **УЧАСТНИК/ПАРТНЕР** должны разработать критерии и признаки сомнительных операций.

УЧАСТНИК/ПАРТНЕР должен осуществлять регулярный мониторинг проводимых операций на предмет выявления сомнительных операций в соответствии с разработанными критериями. При выявлении сомнительных операций, проводимых **КЛИЕНТАМИ**, **УЧАСТНИКОМ/ПАРТНЕРОМ** проводятся мероприятия согласно внутренним документам, разработанным с целью исполнения законодательства в области ПОД/ФТ.

Трудности в выявлении сомнительных операций для **УЧАСТНИКА/ПАРТНЕРА** связаны с тем, что **УЧАСТНИК/ПАРТНЕР** имеет в своем распоряжении информацию только об операциях, проводимых его **КЛИЕНТАМИ**, тогда как **ОПЕРАТОР** владеет полной информацией о перемещении потоков денежных средств и может выявить схемы, реализуемые **КЛИЕНТАМИ**.

С целью предотвращения использования **СИСТЕМЫ** и его **УЧАСТНИКОВ/ПАРТНЕРОВ** в процессе легализации незаконно полученных средств, а также снижения рисков их вовлечения в незаконный оборот наличных денежных средств, **ОПЕРАТОР** устанавливает ограничения на проведение **ПЕРЕВОДОВ** (операций) в рамках **СИСТЕМЫ** и **СЕРВИСА.**

ОПЕРАТОР вправе ввести ограничения на количество **ПЕРЕВОДОВ** (операций) для одного **КЛИЕНТА** (**ПЛАТЕЛЬЩИКА, ПОЛУЧАТЕЛЯ**).

Ограничения, устанавливаемые **ОПЕРАТОРОМ**, могут разрабатываться и действовать в разрезе каждого конкретного **КЛИЕНТА**.

При выявлении **ОПЕРАТОРОМ** операций, которые имеют признаки сомнительности, информация о данных операциях будет доводиться до **УЧАСТНИКА/ПАРТНЕРА** в порядке, указанном в п. 9.

8.1. РАЗРАБОТКА КРИТЕРИЕВ ВЫЯВЛЕНИЯ СОМНИТЕЛЬНЫХ ОПЕРАЦИЙ

При разработке указанных критериев формальный подход недопустим. **ОПЕРАТОР** может указать **УЧАСТНИКУ/ПАРТНЕРУ** на типовые схемы, объемы и состав участников сомнительных операций. Сами же критерии сомнительных операций разрабатываются **УЧАСТНИКОМ/ПАРТНЕРОМ** исходя из индивидуальной практики осуществления переводов денежных средств и с учетом требований национального законодательства в области ПОД/ФТ.

Поэтому очень важно для **УЧАСТНИКА/ПАРТНЕРА**, исходя из сложившейся практики обслуживания **КЛИЕНТОВ**, определить и зафиксировать в своих внутренних документах критерии и признаки сомнительности операций. Эти признаки должны быть по возможности более детальными и содержать информацию о регулярности проведения операций, суммовых порогах, субъектном составе.

Основными критериями сомнительности операций являются их регулярность и объемы.

Крупные объемы переводимых либо получаемых денежных средств **КЛИЕНТАМИ** наряду с регулярностью операций должны привлекать внимание **УЧАСТНИКА/ПАРТНЕРА**. При этом объемы денежных средств, которые будут считаться **УЧАСТНИКОМ/ПАРТНЕРОМ** крупными, определяются каждым **УЧАСТНИКОМ/ПАРТНЕРОМ** самостоятельно исходя из сложившейся практики осуществления **ПЕРЕВОДОВ**.

При разработке критериев **УЧАСТНИКОМ/ПАРТНЕРОМ** также могут быть введены дополнительные факторы отнесения операций к сомнительным. Так, географический фактор может рассматриваться как дополнительный критерий сомнительности операций, к примеру, проведение трансграничных **ПЕРЕВОДОВ** должно привлекать более пристальное внимание **УЧАСТНИКА/ПАРТНЕРА**.

Важным признаком сомнительности операций **КЛИЕНТА** является субъектный состав участников. Особое беспокойство у **УЧАСТНИКА/ПАРТНЕРА** должны вызывать операции совершаемые группой физических лиц.

Так, к примеру, с целью обхода суммовых ограничений **СИСТЕМЫ/СЕРВИСА** по сговору могут действовать несколько физических лиц, проводящих операции в пользу одного и того же получателя. Аналогичные операции могут проводиться и получателями, когда денежные средства перечисляются одним отправителем в пользу группы получателей.

При проведении анализа операций по субъектному составу участников **ОПЕРАТОР** рекомендует выявлять не только операции, в которых фигурируют одни и те же физические лица, но и выявлять системность операций регулярно проводимых отправителем в одном и том же направлении, даже если **ПОЛУЧАТЕЛЯМИ** данных **ПЕРЕВОДОВ** являются различные физические лица.

При возникновении подозрений в том, что операции **КЛИЕНТА** могут быть связаны с предпринимательской деятельностью указанные операции также могут быть отнесены к сомнительным.

8.2. ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ В ЦЕЛЯХ ВЫЯВЛЕНИЯ СОМНИТЕЛЬНЫХ ОПЕРАЦИЙ

Все работники **УЧАСТНИКА/ПАРТНЕРА**, участвующие в осуществлении **ПЕРЕВОДОВ**, должны быть ознакомлены с процедурами, проводимыми

УЧАСТНИКОМ/ПАРТНЕРОМ в целях выявления сомнительных операций. Указанные процедуры должны содержаться во внутренних документах **УЧАСТНИКА/ПАРТНЕРА** и неукоснительно выполняться работниками при выявлении сомнительных операций.

Работники, непосредственно обслуживающие **КЛИЕНТОВ**, в рамках прохождения обучения знакомятся со схемами, признаками и критериями, разработанными **УЧАСТНИКОМ/ПАРТНЕРОМ** для выявления сомнительных операций.

Чтобы иметь возможность на месте при обслуживании **КЛИЕНТА** оценить уровень риска проведения **КЛИЕНТОМ** сомнительных операций работник **УЧАСТНИКА/ПАРТНЕРА** должен обладать знаниями относительно типовых схем сомнительных операций.

ОПЕРАТОР имеет возможность выявить сомнительные операции **КЛИЕНТОВ** по ряду формальных признаков, однако существуют признаки, которые **ОПЕРАТОР** оценить не в силах, в таких случаях ключевым становится участие работника **УЧАСТНИКА/ПАРТНЕРА**, обслуживающего **КЛИЕНТА**.

Только работники **УЧАСТНИКА/ПАРТНЕРА** на месте при непосредственном контакте с **КЛИЕНТОМ** для отнесения операций к сомнительным могут основываться на таких неформальных признаках как поведение **КЛИЕНТА**, проявление излишней озабоченности при проведении операции.

Излишняя озабоченность **КЛИЕНТА** вопросами конфиденциальности проводимых операций, а также заинтересованность в уклонении от процедуры идентификации являются для работника **УЧАСТНИКА/ПАРТНЕРА** дополнительными показателями сомнительности операций.

Дополнительным поводом для повышенного внимания к операциям **КЛИЕНТА** является нежелание **КЛИЕНТА** предоставить сведения и документы по просьбе работника **УЧАСТНИКА/ПАРТНЕРА**, предоставление которых не предусмотрено законодательством, но в рамках сложившейся банковской практики запрашиваемых у **КЛИЕНТА**.

Как уже упоминалось, главным признаком сомнительности операций является их регулярность, поэтому при частом обращении **КЛИЕНТА** в течение короткого периода времени (одного или нескольких операционных дней) для оказания ему услуги по переводу денежных средств без открытия счета у работника **УЧАСТНИКА/ПАРТНЕРА** могут возникнуть сомнения относительно законности проводимых операций.

Регулярность проводимых операций особенно должна привлекать внимание работника **УЧАСТНИКА/ПАРТНЕРА** в случае если **КЛИЕНТОМ** проводятся операции на суммы равные суммовым ограничениям Системы либо близкие к ним.

Контроль на предмет выявления сомнительных операций должен проводиться **УЧАСТНИКОМ/ПАРТНЕРОМ**, как в разрезе **ПЛАТЕЛЬЩИКОВ**, так и **ПОЛУЧАТЕЛЕЙ**.

В случае если **УЧАСТНИК/ПАРТНЕР**, обслуживающий **ПОЛУЧАТЕЛЯ**, при анализе операций выявляет систематичность **ПЕРЕВОДОВ**, приходящих в адрес одного и того же **КЛИЕНТА** (как **ПЕРЕВОДЫ** от одного, так и нескольких **ПЛАТЕЛЬЩИКОВ**, как **ПЕРЕВОДЫ,** отправляемые из одного направления, так и **ПЕРЕВОДЫ** из различных направлений), то такие операции могут быть расценены как связанные с предпринимательской деятельностью.

В случае выявления **УЧАСТНИКОМ/ПАРТНЕРОМ**, обслуживающим **ПЛАТЕЛЬЩИКА**, регулярных **ПЕРЕВОДОВ КЛИЕНТОМ** в адрес физических лиц в различные направления можно сделать вывод об отсутствии какого бы то ни было экономического смысла в данных операциях и, следовательно, классифицировать их как сомнительные.

Также при проведении операций **КЛИЕНТА**, которые, по мнению работника **УЧАСТНИКА/ПАРТНЕРА**, имеют признаки сомнительности, работником **УЧАСТНИКА/ПАРТНЕРА** могут быть запрошены документы, необходимые для классификации операции. К примеру, документы подтверждающие источники происхождения денежных средств **КЛИЕНТА**, а также экономический смысл проводимых операций.

Отказ от предоставления **КЛИЕНТОМ** указанных документов может являться для **УЧАСТНИКА/ПАРТНЕРА** причиной для отказа **КЛИЕНТУ** в поведении его операций. В случае если **УЧАСТНИК/ПАРТНЕР** проводит операции **КЛИЕНТА** на крупные суммы, то **СИСТЕМА/СЕРВИС** принимает, что **УЧАСТНИКОМ/ПАРТНЕРОМ** были проведены соответствующие мероприятия и у **УЧАСТНИКА/ПАРТНЕРА** есть основания не относить операции **КЛИЕНТА** к разряду сомнительных.

Работники **УЧАСТНИКА/ПАРТНЕРА** также могут прибегнуть к помощи службы безопасности **УЧАСТНИКА/ПАРТНЕРА**, которая помимо проверки благонадежности **КЛИЕНТА** может помочь сотрудникам сделать вывод об использовании **КЛИЕНТОМ** инструмента **ПЕРЕВОДОВ** в целях осуществления предпринимательской деятельности.

Помимо перечисленных мероприятий во внутренних документах **УЧАСТНИКА/ПАРТНЕРА** могут содержаться дополнительные меры, принимаемые сотрудниками для выявления сомнительных операций.

Итогом всех проводимых мероприятий является заключение Ответственного сотрудника **УЧАСТНИКА/ПАРТНЕРА** об отнесении операций, проводимых **КЛИЕНТОМ**, к необычными, либо признание их экономически обоснованными.

Соответственно, принимается решение о дальнейшем обслуживании **КЛИЕНТА** либо об отказе в совершении его операций.

9. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СИСТЕМЫ С УЧАСТНИКАМИ/ПАРТНЕРАМИ

Направление деятельности **СИСТЕМЫ** в части разработки общих принципов подхода к построению системы противолегализационного контроля, применяемых всеми ее **УЧАСТНИКАМИ/ПАРТНЕРАМИ**, являются исходными пунктами в эффективной борьбе против отмывания денег.

Для работы в рамках **СИСТЕМЫ УЧАСТНИКУ** необходимо представить сведения о принимаемых им мерах по ПОД/ФТ.

СИСТЕМА не устанавливает и не поддерживает отношений с **УЧАСТНИКАМИ/ПАРТНЕРАМИ**, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления, а также **УЧАСТНИКАМИ/ПАРТНЕРАМИ**, в отношении которых имеется информация, что их счета используются банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления.

Также для поддержания информации о **УЧАСТНИКАХ** в актуальном виде **РАСЧЕТНЫМ ЦЕНТРОМ** на регулярной основе проводится обновление данных об **УЧАСТНИКАХ**В рамках взаимодействия **СИСТЕМЫ** и **УЧАСТНИКОВ/ПАРТНЕРОВ** осуществляются мероприятия, направленные на выявление сомнительных операций.

Для создания эффективных способов функционирования системы по выявлению сомнительных операций необходимо иметь единый источник методических рекомендаций, роль которого на себя принимает **СИСТЕМА**.

СИСТЕМА оказывает **УЧАСТНИКАМ/ПАРТНЕРАМ** помощь в выявлении сомнительных операций и для этого доводит до них информацию об операциях, осуществляемых **КЛИЕНТАМИ УЧАСТНИКОВ/ПАРТНЕРОВ**.

СИСТЕМЕ более очевидны схемы, используемые **КЛИЕНТАМИ** при проведении операций, поскольку в ее распоряжении находятся данные о консолидированных потоках денежных средств.

Отдельные операции, совершаемые **КЛИЕНТОМ**, для работника **УЧАСТНИКА/ПАРТНЕРА** в момент проведения операции могут не иметь признаков сомнительности, тогда как на уровне **СИСТЕМЫ**, при возможности проведения комплексного анализа операций и со стороны плательщика, и со стороны получателя эти операции могут быть рассмотрены как сомнительные.

Критерии, согласно которым **СИСТЕМА** принимает решение об отнесении операций к разряду сомнительных, не разглашаются в целях сохранения их актуальности.

9.1. ДОВЕДЕНИЕ ДО УЧАСТНИКОВ/ПАРТНЕРОВ ИНФОРМАЦИИ ОБ ОПЕРАЦИЯХ, ИМЕЮЩИХ ПРИЗНАКИ СОМНИТЕЛЬНОСТИ

При выявлении операций, которые на основании их объемов, регулярности и

персонального состава можно отнести к сомнительным, информация о них доводится до Ответственных сотрудников **УЧАСТНИКОВ/ПАРТНЕРОВ**.

СИСТЕМА предлагает Ответственным сотрудникам **УЧАСТНИКОВ/ПАРТНЕРОВ** воспользоваться информацией о **ПЕРЕВОДАХ** (операциях) **КЛИЕНТА**, которую можно получить в программно-аппаратном комплексе **СИСТЕМЫ** в виде ежедневного отчета.

Факт направления **СИСТЕМОЙ** в адрес **УЧАСТНИКА/ПАРТНЕРА** информации об операциях **КЛИЕНТА** не означает, что **КЛИЕНТУ** необходимо отказать в обслуживании, либо операции **КЛИЕНТА** необходимо отнести к разряду необычных. Выявленные **СИСТЕМОЙ** операции лишь формально подпадают под признаки сомнительности, разработанные **СИСТЕМОЙ**.

Окончательное решение о признании операций **КЛИЕНТА** необычными принимается Ответственным сотрудником **УЧАСТНИКА/ПАРТНЕРА** на основании критериев, разработанных в соответствии со спецификой деятельности кредитной организации.

Доведение информации об операциях, имеющих признаки сомнительности, осуществляется как для **УЧАСТНИКА/ПАРТНЕРА**, обслуживающего **ПЛАТЕЛЬЩИКА**, так и для **УЧАСТНИКА/ПАРТНЕРА**, обслуживающего **ПОЛУЧАТЕЛЯ**.

9.2. ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПРИ ВЫЯВЛЕНИИ СОМНИТЕЛЬНЫХ ОПЕРАЦИЙ

Наряду с информацией об операциях **КЛИЕНТОВ СИСТЕМОЙ** могут быть доведены до **УЧАСТНИКА/ПАРТНЕРА** рекомендации с указанием мер, которые, в случае признания операций необычными, можно применить к указанному **КЛИЕНТУ** в целях прекращения таких операций.

Меры, применяемые **УЧАСТНИКОМ/ПАРТНЕРОМ** к операциям **КЛИЕНТА**, должны быть описаны во внутренних документах **УЧАСТНИКА/ПАРТНЕРА**.

В случае признания операций **КЛИЕНТА** сомнительными **УЧАСТНИКОМ/ПАРТНЕРОМ** могут быть запрошены у **КЛИЕНТА** дополнительные документы в целях пояснения источников происхождения денежных средств, а также обоснования законности проводимых операций.

Также работниками **УЧАСТНИКА/ПАРТНЕРА** могут быть приняты дополнительные меры, к примеру, представителем службы безопасности **УЧАСТНИКА/ПАРТНЕРА** может быть составлена беседа с **КЛИЕНТОМ**.

В случае если после доведения информации **УЧАСТНИК/ПАРТНЕР** продолжает проводить операции указанного **КЛИЕНТА**, **СИСТЕМА** считает, что **УЧАСТНИКОМ/ПАРТНЕРОМ** были проведены необходимые мероприятия, и в операциях **КЛИЕНТА** не было выявлено сомнительности.

При признании Ответственным сотрудником **УЧАСТНИКА/ПАРТНЕРА** операций **КЛИЕНТА** необычными информацию о выявленных операциях необходимо довести до органов национальной финансовой разведки.

В органы финансовой разведки, как правило, необходимо представлять информацию о **КЛИЕНТЕ** в полном объеме, для этого необходимо провести идентификацию **КЛИЕНТА** согласно п. 7.4.

Также **УЧАСТНИК/ПАРТНЕР** обязан принять меры для прекращения проведения указанных операций.

9.3. ПОРЯДОК РАБОТЫ СО «СПИСКОМ СОМНИТЕЛЬНЫХ КЛИЕНТОВ»

В целях прекращения проведения необычных операций **УЧАСТНИК/ПАРТНЕР** может воспользоваться таким инструментом как «Список сомнительных клиентов».

В случае если операции **КЛИЕНТА** были признаны **УЧАСТНИКОМ/ПАРТНЕРОМ** необычными, **УЧАСТНИК/ПАРТНЕР** может обратиться к **ОПЕРАТОРУ** с просьбой о включении данного **КЛИЕНТА** в Список.

КЛИЕНТ может быть включен в Список только в том случае, если основания, приведенные **УЧАСТНИКОМ/ПАРТНЕРОМ**, будут признаны **ОПЕРАТОРОМ** достаточными.

При возникновении ситуации, когда для осуществления **ПЕРЕВОДА** к **УЧАСТНИКУ/ПАРТНЕРУ** обращается **КЛИЕНТ**, данные которого совпадают с данными содержащимися в «Списке сомнительных клиентов», **СИСТЕМА** информирует об этом сотрудника **УЧАСТНИКА/ПАРТНЕРА** через программно-аппаратный комплексе **СИСТЕМЫ** в виде сообщения. Распоряжение **КЛИЕНТА** на **ПЕРЕВОД** в указанном случае не принимается к исполнению.

ОПЕРАТОР вправе включать **КЛИЕНТА** в «Список сомнительных клиентов» самостоятельно.

В «Список сомнительных клиентов» могут быть включены **КЛИЕНТЫ**, как **ПЛАТЕЛЬЩИКИ**, так и **ПОЛУЧАТЕЛИ**.

9.3.1. ПОРЯДОК ВКЛЮЧЕНИЯ КЛИЕНТА В «СПИСОК СОМНИТЕЛЬНЫХ КЛИЕНТОВ» ПО ИНИЦИАТИВЕ УЧАСТНИКА/ПАРТНЕРА

Включение клиента в «Список сомнительных клиентов» по инициативе **УЧАСТНИКА/ПАРТНЕРА** происходит на основании представления **УЧАСТНИКА/ПАРТНЕРА** в письменной форме за подписью руководителя **УЧАСТНИКА/ПАРТНЕРА**.

УЧАСТНИКОМ/ПАРТНЕРОМ перечисляются обстоятельства, на основании которых было принято решение об отнесении операций **КЛИЕНТА** к сомнительным. В случае необходимости, прикладываются документы, являющиеся основанием для принятия такого решения.

Для включения в Список необходимо однозначно установить личность **КЛИЕНТА**, соответственно, **УЧАСТНИКУ/ПАРТНЕРУ** необходимо провести

идентификацию **КЛИЕНТА** в полном объеме.

В случае признания **ОПЕРАТОРОМ** изложенных обстоятельств достаточными для включения **КЛИЕНТА** в «Список сомнительных клиентов», **КЛИЕНТ** включается в Список.

После включения **КЛИЕНТА** в Список **ПЕРЕВОДЫ** по распоряжению **КЛИЕНТА** не проводятся в течение 1 года.

9.3.2. ПОРЯДОК ИСКЛЮЧЕНИЯ КЛИЕНТА ИЗ «СПИСКА СОМНИТЕЛЬНЫХ КЛИЕНТОВ»

ПЕРЕВОДЫ по распоряжению **КЛИЕНТОВ**, включенных в «Список сомнительных клиентов», по истечении 1 года могут быть проведены.

По истечении 1 года **КЛИЕНТ** автоматически исключается из «Списка сомнительных клиентов». Для этого не требуется проведения каких либо мероприятий со стороны **УЧАСТНИКА/ПАРТНЕРА**.

После исключения **КЛИЕНТА** из Списка, его распоряжения на **ПЕРЕВОДЫ** проводятся на общих основаниях.

10. ПОРЯДОК ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Ответственный сотрудник **УЧАСТНИКА/ПАРТНЕРА** принимает на себя обязанность по созданию и мониторингу функционирования в Банке эффективной системы внутреннего контроля, включая обеспечение конфиденциальности информации.

На Ответственном сотруднике **УЧАСТНИКА/ПАРТНЕРА** лежит обязанность по проведению разъяснительной работы с работниками. Работники **УЧАСТНИКА/ПАРТНЕРА**, обслуживающие **КЛИЕНТА**, должны знать, что информация о мерах, предпринимаемых Банком в целях ПОД/ФТ, является конфиденциальной и не подлежит разглашению, как **КЛИЕНТА**, так и третьим лицам.

Также работники **УЧАСТНИКА/ПАРТНЕРА** должны осознавать необходимость соблюдения конфиденциальности в отношении операций, проводимых **КЛИЕНТАМИ**, а также персональных данных **КЛИЕНТОВ**.

10.1. ЗАПРЕТ НА ИНФОРМИРОВАНИЕ КЛИЕНТА И ТРЕТЬИХ ЛИЦ О МЕРОПРИЯТИЯХ, ПРОВОДИМЫХ В ЦЕЛЯХ ПОД/ФТ

Настоящая **ПОЛИТИКА**, как и внутренние документы **УЧАСТНИКА/ПАРТНЕРА** по ПОД/ФТ являются документами ограниченного использования и не подлежат публичному распространению.

Работники **УЧАСТНИКА/ПАРТНЕРА** не имеют права информировать, кого бы то ни было о мероприятиях, проводимых в целях ПОД/ФТ. Также работникам **УЧАСТНИКА/ПАРТНЕРА** запрещается консультировать **КЛИЕНТА** о возможностях уклонения от процедур, предусмотренных **ПОЛИТИКОЙ**.

Все работники **УЧАСТНИКА/ПАРТНЕРА**, вовлеченные в проведение операций, должны иметь представление об ответственности за ненадлежащее исполнение мероприятий в области ПОД/ФТ в соответствии с законодательством страны, резидентом которой является **УЧАСТНИК/ПАРТНЕР**.

Информация о **КЛИЕНТЕ** и о проводимых им операциях может быть предоставлена только самому **КЛИЕНТУ** либо его представителю. Также указанная информация может предоставляться государственным органам по их запросам только в случаях предусмотренных законодательством.

10.2. СОБЛЮДЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ОБ ОПЕРАЦИЯХ КЛИЕНТОВ

СИСТЕМА/СЕРВИС гарантирует соблюдение тайны относительно операций, совершаемых в рамках **СИСТЕМЫ/СЕРВИСА**. Работники **УЧАСТНИКА/ПАРТНЕРА** также обязаны сохранять тайну операций своих **КЛИЕНТОВ**.

При взаимодействии с **УЧАСТНИКАМИ/ПАРТНЕРАМИ СИСТЕМА/СЕРВИС**

руководствуется нормами законодательства о неразглашении банковской тайны и предоставляет информацию об операциях **КЛИЕНТОВ** в том объеме, которым владеет **УЧАСТНИК/ПАРТНЕР**.

К примеру, при направлении информации об операциях **ПЛАТЕЛЬЩИКА** в **БАНК ПЛАТЕЛЬЩИКА, СИСТЕМА/СЕРВИС** предоставит относительно **ПОЛУЧАТЕЛЯ** информацию только в том объеме, которым владеет **БАНК ПЛАТЕЛЬЩИКА**. Как правило, это информация о фамилии, имени, отчестве **ПОЛУЧАТЕЛЯ** и направлении **ПЕРЕВОДА**. Аналогично и в случае предоставления **СИСТЕМОЙ/СЕРВИСОМ** информации об операциях **ПОЛУЧАТЕЛЯ** в адрес **БАНКА ПЛАТЕЛЬЩИКА**.

В случае разглашения сведений, составляющих банковскую тайну, виновные лица несут ответственность согласно национальному законодательству.

10.3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА

Также **СИСТЕМА/СЕРВИС** гарантирует конфиденциальность персональных данных, предоставленных **КЛИЕНТАМИ**, и требует от **УЧАСТНИКОВ/ПАРТНЕРОВ** соблюдения данного условия.

УЧАСТНИКАМИ/ПАРТНЕРАМИ должны быть приняты организационные и технические меры для обеспечения защиты получаемых персональных данных **КЛИЕНТОВ**.

Персональные данные, полученные при проведении идентификации **КЛИЕНТА**, не подлежат передаче третьим лицам без согласия самого **КЛИЕНТА**.

Персональные данные **КЛИЕНТА** могут быть предоставлены органам государственной власти либо иным субъектам, имеющим на это право при наличии на то законных оснований.