

«УТВЕРЖДЕНО»
Наблюдательным советом АКБ
«Капиталбанк»

«27» октября 2022 года

(протокол № 48)

Председатель Совета банка

_____ Абдусаматов М.А.



ПОЛИТИКА
ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ,
ПОЛУЧЕННЫХ ОТ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ,
И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА ИЛИ
ФИНАНСИРОВАНИЮ РАСПРОСТРАНЕНИЯ ОРУЖИЯ
МАССОВОГО УНИЧТОЖЕНИЯ
В АКБ «КАПИТАЛБАНК»
(новая редакция)

ПРЕАМБУЛА

Учитывая важность и особую значимость проводимой во всем цивилизованном мире политики по противодействию легализации преступных доходов, в том числе учитывая угрозу, исходящую для всего мирового сообщества от террористических и связанных с ними организаций, а также в целях предотвращения угрозы отмыывания преступных денег и эффективное выявление и пресечение операций, направленных на легализацию преступных доходов, недопущение умышленного или неумышленного вовлечения банка в преступную деятельность и обеспечение неукоснительного соблюдения требований законодательства о противодействии легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Капиталбанк» (далее – банк) разработан и введен в действие комплекс мероприятий, направленных на своевременное выявление сомнительных и подозрительных операций.

Банком предпринимаются все возможные меры по предотвращению операций и сделок, которые прямо или косвенно связаны с отмыыванием доходов, полученных от преступной деятельности, а также по исключению возможности проведения операций, связанных с финансированием террористической деятельности или финансированием распространения оружия массового уничтожения.

Банк с осторожностью подходит к выбору и формированию своей клиентской базы по принципу «Знай своего клиента», внимательно изучает своих клиентов, интересы и сферы их деятельности и стремится к установлению взаимоотношений, основанных на прозрачности и понимании бизнеса и операций клиентов.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения в АКБ «Капиталбанк» (далее – Политика) разработана в соответствии с законами Республики Узбекистан «О банках и банковской деятельности», «О банковской тайне», «О противодействии легализации доходов, полученных от преступной деятельности, и финансированию терроризма», а также Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в коммерческих банках (рег.: Минюст за № 2886 от 23.05.2017 г.), Положением о минимальных требованиях, предъявляемых к деятельности коммерческих банков при осуществлении взаимоотношений с потребителями банковских услуг (рег.: Минюст за № 3030 от 02.07.2018 г.), а также рекомендациями Группы (межправительственной комиссии) по разработке финансовых мер по борьбе с отмыыванием денег (ФАТФ).

2. Процедуры и правила, указанные в настоящей Политике, являются предметом изменений и дополнений, в соответствии с изменениями законодательной базы Республики Узбекистан и международных норм, и стандартов.

3. В настоящей Политике используются следующие основные понятия:

Внутренние правила ПОД/ФТ и ФРОМУ – Правила внутреннего контроля по легализации преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения в АКБ «Капиталбанк» (новая редакция);

ФАТФ – Межправительственная комиссия по борьбе с отмыыванием криминальных капиталов, которая занимается выработкой мировых стандартов в сфере противодействия легализации преступных доходов и финансированию терроризма, а также осуществляет оценки соответствия национальных систем противодействия легализации преступных доходов и финансированию терроризма этим стандартам;

легализация доходов, полученных от преступной деятельности – уголовно наказуемое общественно опасное деяние, представляющее собой придание правомерного вида происхождению собственности (денежных средств или иного имущества) путем ее перевода, превращения или обмена, а равно сокрытие либо утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, подлинных прав в отношении денежных средств или иного имущества либо его принадлежности, если денежные средства или иное имущество получено в результате преступной деятельности;

финансирование терроризма – уголовно наказуемое общественно опасное деяние, направленное на обеспечение существования, функционирования, финансирования террористической организации, выезда за границу либо передвижения через территорию Республики Узбекистан для участия в террористической деятельности, подготовку и совершение террористической акции, прямое или косвенное предоставление или сбор любых средств, ресурсов, иных услуг террористическим организациям либо лицам, содействующим или участвующим в террористической деятельности;

финансирование распространения оружия массового уничтожения – предоставление или сбор любых средств, ресурсов, иных услуг в целях разработки, производства, приобретения, накопления, хранения, сбыта, использования ядерного, химического, биологического и других видов оружия массового уничтожения, материалов и оборудования, которые заведомо могут быть использованы при его создании;

перечень – перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, формируемый специально уполномоченным государственным органом на основании сведений, представляемых государственными органами, осуществляющими борьбу с терроризмом, распространением оружия массового уничтожения, и другими компетентными органами Республики Узбекистан, а также сведений, полученных по официальным каналам от компетентных органов иностранных государств и международных организаций;

процесс эскалации – процесс передачи решения по установлению деловых связей с рисковыми Клиентами или ПДЛ/ГДЛ/ГС высшему руководству или службам, которые отвечают за риски по ПОД/ФТ и ФРОМУ и ставят соответствующие задачи перед работниками и бизнесом;

принцип «четырёх глаз» – принцип предусматривает, что для выполнения задачи внутреннего контроля требуется не менее двух сотрудников. Целью принципа является защита от внутреннего мошенничества и предотвращение единоличного контроля. Термин также упоминается как «двойной контроль», «maker-checker» или «правило двух человек»;

риск – риск совершения клиентами операций в целях легализации доходов, полученных от преступной деятельности, или финансирования терроризма;

департамент комплаенс контроля банка – структурное подразделение банка, ответственное за осуществление внутреннего контроля в целях ПОД/ФТ и ФРОМУ и приведение деятельности банка в соответствие с требованиями законодательства;

ответственный сотрудник – сотрудник банка, ответственный за соблюдение банком правил внутреннего контроля в целях ПОД/ФТ и ФРОМУ и предоставление сведений в специально уполномоченный государственный орган в лице Департамента по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан;

особые сферы/отрасли бизнеса – индустрии/сектора, сферы деятельности Клиентов (включая индустрию азартных игр, криптовалюты, развлечений для взрослых, поставщиков платежных/денежных услуг и другие), в отношении которых Банк устанавливает ограничительные меры, связанные с требованиями законодательства. Взаимодействие с особыми сферами/отраслями бизнеса может быть приемлемо для Банка при наличии средств контроля, установленных клиентом и/или Банком;

азартные игры (игорный бизнес) – особая сфера/отрасль бизнеса, игры основанные на риске, предусматривающие совокупность действий ее организаторов и участников в соответствии с основанным на риске соглашением, заключенным организатором игры (игорного заведения) с одним или более участниками о выигрыше, который зависит от случая

(события) и (или) от способностей, ловкости и других качеств участника игры, в том числе тотализаторы, казино, а также игра с использованием игровых автоматов. К игорному бизнесу относятся предприятия с физическим местонахождением (например, казино, букмекерские конторы, операторы игровых автоматов), производители игорного оборудования, удаленные и онлайн игорные предприятия, а также поставщики программного обеспечения для азартных игр и хостинга;

криптовалюты (децентрализованные виртуальные валюты) – это распределенные, с открытым исходным кодом, P2P, виртуальные валюты, средство цифрового выражения стоимости, которое не выпускается центральным банком или государственным органом и необязательно привязано к официальной валюте, которое не обладает законным статусом валюты или денег, но которое принимается в качестве средства обмена и может переводиться, храниться, покупаться и продаваться в электронном виде.

развлечения для взрослых – любое предприятие, в которое не допускаются несовершеннолетние, которое продает, сдает в аренду или демонстрирует сексуально откровенные материалы или другие подобные действия;

услуги по переводу денег или ценностей / предоставлению платежей (УПДЦ) – услуги, предоставляемые небанковскими организациями, которые включают прием наличных денег, чеков, или других средств сбережения и выплату соответствующей суммы в наличной или иной форме бенефициару посредством связи, сообщения, перевода или через клиринговую сеть, к которой принадлежит провайдер УПДЦ. Транзакции, выполняемые такими службами, могут включать одного или нескольких посредников и окончательный платеж третьей стороне, а также могут включать любые новые способы оплаты;

клиент – физическое/юридическое лицо/индивидуальный предприниматель, намеревающееся инициировать деловые отношения с банком, или уже находящееся на обслуживании в банке, либо осуществляющее разовую сделку с банком от своего имени в своих интересах, либо в интересах третьих лиц;

участники операции – клиенты, их представители, а также партнеры/контрагенты клиента участвующие в операции;

третья сторона – организации, осуществляющие операции с денежными средствами или иным имуществом;

бенефициарный собственник – лицо, которое в конечном итоге владеет правами собственности или реально контролирует клиента, и в интересах которого совершается операция с денежными средствами или иным имуществом;

идентификация бенефициарного собственника клиента – определение банком юридического лица собственника, в том числе лица контролирующего клиента путем изучения структуры собственности и управления на основании учредительных документов, определенных законодательством (устава и (или) учредительного договора, положения);

публичные должностные лица (ПДЛ) – лица, назначаемые или избираемые постоянно, временно или по специальному полномочию, выполняющие организационно-распорядительные функции в государственных органах и уполномоченные на совершение юридически значимых действий а также лица, осуществляющие указанные функции международной организации либо в законодательном, исполнительном, административном или судебном органе иностранного государства;

государственное должностное лицо (ГДЛ)/государственный служащий (ГС) – гражданин Республики Узбекистан, занимающий важную должность в государственном органе Республики Узбекистан, которому доверены или были доверены, значительные политические функции, например, главы государств или правительств, видные политики, старшие правительственные, судебные или военные сотрудники, старшие руководители государственных корпораций, видные деятели политических партий;

близкие родственники ПДЛ/ГДЛ/ГС – физические лица, которые связаны с ПДЛ/ГДЛ/ГС напрямую (кровное родство) или браком или схожие (гражданские) формы партнерства;

близкие к ПДЛ/ГДЛ/ГС лица – физические лица, которые тесно связаны с ПДЛ/ГДЛ/ГС социально или профессионально;

специально уполномоченный государственный орган (далее – **СУГО**) – Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан;

филиал – филиалы, Центры банковских услуг, ОПЕРУ, ЦОО АКБ «Капиталбанк».

ГЛАВА 2. ОСНОВНЫЕ ПРИНЦИПЫ

4. В целях предотвращения вовлечения банка в проведение операций, связанных с отмыванием доходов, полученных от преступной деятельности, и финансированием терроризма или финансированием распространения оружия массового уничтожения, банк руководствуется следующими основными принципами:

следовать общим подходам, изложенным в настоящей политике, при создании и совершенствовании системы внутреннего контроля в целях противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

разрабатывать собственные правила внутреннего контроля в целях противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения на основе национального законодательства и настоящей политики;

предпринимать действия, направленные на определение, оценки и снижение рисков, связанных с вовлечением Банка в схемы по ОД/ФТ и ФРОМУ при проведении всех банковских операций, в том числе валютных операций, доведение услуг Банка до клиентов, установлений корреспондентских отношений, а также разработка и внедрение новых видов услуг, технологии и продуктов.

ГЛАВА 3. ОСНОВНЫЕ ЗАДАЧИ

5. Основными задачами по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма являются:

а) организация эффективной системы внутреннего контроля по выявлению операций, подлежащих сообщению в СУГО, во всех подразделениях и филиалах Банка;

б) эффективное выявление и пресечение операций с денежными средствами или иным имуществом, направленных на легализацию доходов, полученных от преступной деятельности, и финансирование терроризма или финансирование распространения оружия массового уничтожения;

в) недопущение умышленного или неумышленного вовлечения Банка в преступную деятельность, проникновения преступного капитала в его уставный фонд (капитал), а также проникновения преступных лиц в управление Банком;

г) обеспечение неукоснительного соблюдения требований законодательства о противодействии легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения;

д) изучение системы внутреннего контроля других Банков республики Узбекистан и иностранных Банков при установлении с ними корреспондентских отношений.

ГЛАВА 4. ОТВЕТСТВЕННЫЙ СОТРУДНИК БАНКА

6. Учитывая, что Банк осуществляет различные виды операций (расчетные, кассовые, депозитные, валютные, кредитные операции и т. п.), за реализацию данной политики отвечают руководители структурных подразделений и руководство филиалов, непосредственно вовлеченные в эти процессы, а общее кураторство и контроль осуществляет ответственный сотрудник (являющийся директором департамента комплаенс контроля,

который руководит деятельностью закрепленных сотрудников за филиалами), одобренный Наблюдательным советом и назначаемый приказом председателя Правления Банка.

7. Директор Департамента комплаенс контроля, является независимым при принятии решений и выполнении своих должностных обязанностей.

Директор Департамента комплаенс контроля обладает «правом вето» в отношении установления деловых отношений с клиентом и открытия банковского счета, проведения сделок или транзакций, направленных на легализацию доходов, полученных от преступной деятельности и финансирования терроризма и распространения оружия массового уничтожения.

8. Ответственный сотрудник должен быть достаточно авторитетным, корректным, честным и справедливым.

9. В обязанности ответственного сотрудника входят:

обеспечение осведомленности других сотрудников Банка о политике по недопущению отмывания доходов, полученных преступным путем;

осуществление проверок на предмет исполнения процедур, предусмотренных правилами по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в Банке и мониторинг за устранением выявленных нарушений;

ведение записей, архивация и сохранение соответствующей информации и документации в отношении транзакций, затронутых правилами по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения;

принятие действенных мер на основании критериев, предусмотренных внутренними правилами по легализации доходов, полученных от преступной деятельности, и финансированию терроризма в случаях обнаружения подозрительных операций;

согласно требованиям законов Республики, Узбекистан установление контактов с уполномоченными органами по соблюдению исполнения законодательства по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

ГЛАВА 5. ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ

10. Основным способом эффективного предотвращения отмывания доходов, полученных преступным путем, является надлежащая проверка клиента. Надлежащая проверка осуществляется на основании информации и документов, предоставляемых клиентами Банка, и включает принцип «четырёх глаз» (проверка со стороны двух сотрудников) в отношении идентификации документов клиента и другой информация надлежащей проверки клиента.

Процесс эскалации (сроки, периодичность, пошаговая инструкция, ответственные лица и т. д.) проведения надлежащей проверки клиента регламентирован в локальных актах по обслуживанию физических и юридических лиц.

11. Банк самостоятельно принимает меры по надлежащей проверке клиентов в следующих случаях:

а) при установлении хозяйственных и гражданско-правовых отношений, в том числе: при обращении юридического или физического лица с заявлением на открытие банковского счета (вклада);

при обращении физического лица с заявлением на получение банковской карты;

при обращении юридических и (или) физических лиц с заявлением на приобретение ценных бумаг, эмитированных коммерческим Банком;

при владении юридическими и (или) физическими лицами акциями коммерческого Банка, на сумму, равную или превышающую один процент его уставного капитала;

при обращении физического лица за получением кредита или услуги по хранению ценностей в банковской депозитной ячейке;

б) при осуществлении разовых операций, в том числе путем совершения одной или нескольких операций, связанных между собой, в случаях:

получения клиентами из банковской кассы наличной иностранной валюты по банковским картам, эмитированным другими Банками, на сумму, равную или превышающую 100-кратный размер базовой расчетной величины;

покупки физическими лицами иностранной валюты в размере, превышающем 100 долларов США в эквиваленте;

осуществления операции без открытия или использования банковского счета на сумму, равную или превышающую 500-кратный размер базовой расчетной величины;

при совершении или получении денежных переводов, предусмотренных абзацем первым пункта 34-1, Правила внутреннего контроля АКБ Капиталбанка;

в) при наличии подозрений в легализации доходов, полученных от преступной деятельности, и финансировании терроризма независимо от любых исключений, установленных Правилами внутреннего контроля АКБ Капиталбанка;

г) при наличии сомнений относительно достоверности или достаточности ранее полученных данных о клиенте.

12. Меры по надлежащей проверке клиента, принимаемые Банком, осуществляются в соответствии с внутренними правилами ПОД/ФТ и ФРОМУ Банка и обязательно включают:

а) проверку личности и полномочий клиента и лиц, от имени которых он действует на основании соответствующих документов;

б) идентификацию бенефициарного собственника клиента;

в) изучение цели и характера деловых отношений или запланированных операций;

г) проверку достоверности и обновление сведений о клиенте, лиц, действующих от имени клиента и бенефициарном собственнике;

г) проведение на постоянной основе изучения деловых отношений и операций, осуществляемых клиентом, в целях проверки их соответствия сведениям о таком клиенте и его деятельности.

Помимо применения вышеуказанных мер по надлежащей проверке клиента, в отношении ПДЛ/ГДЛ/ГС, выступающих в качестве клиента или бенефициарного собственника клиента, Банк должен:

применять разумные меры для проверки сведений о статусе ПДЛ/ГДЛ/ГС и определения источника денежных средств или иного имущества по операции;

устанавливать деловые отношения с ПДЛ только с разрешения председателя Правления Банка или его уполномоченного заместителя;

осуществлять постоянный углубленный мониторинг деловых отношений.

13. Банк может доверять результатам надлежащей проверки клиента, проведенной третьими сторонами, по мерам надлежащей проверки, указанным в абзацах а) и в) - пункта 12 настоящей Политики. В таких случаях конечную ответственность по надлежащей проверке клиента несет сам Банк. При этом Банк должен удостовериться:

в возможности незамедлительного получения (посредством электронных систем) необходимой информации по надлежащей проверке клиентов;

в возможности по запросу незамедлительного получения копий идентификационных данных и других соответствующих документов по надлежащей проверке клиентов;

в том, что третьи стороны руководствуются внутренними правилами по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения.

В случае несоблюдения одного из требований, предусмотренных в абзацах втором и четвертом настоящего пункта, Банк должен самостоятельно принимать меры по надлежащей проверке клиентов.

Банк принимает решение о вступлении в деловые отношения с клиентом самостоятельно, исходя из риска, а также вправе принимать меры по надлежащей проверке.

Банк должен оговорить о возможности принятия мер по надлежащей проверке клиентов в договоре и (или) в договоре оферты.

14. Все документы, позволяющие идентифицировать клиента и иных участников операции должны быть действительными на дату их предъявления. Документы, составленные на иностранном языке (полностью, или в какой-либо части), представляются в Банк с заверенным в установленном порядке переводом на государственный или русский язык, и в случае необходимости, легализованным.

15. Банк, при наличии подозрений в достоверности полученной информации и документов, должен осуществлять меры по проверке (верификации) этой информации и этих документов. В таком случае, Банк вправе обращаться в соответствующие организации с запросом для выяснения достоверности (подлинности) информации и документов о клиентах. Также, Банк вправе потребовать представления подлинников документов для ознакомления, в случае возникновения сомнений в достоверности представленных копий документов.

16. Банк вправе отказать клиенту в осуществлении операции с денежными средствами или иным имуществом в случае:

- отсутствия по своему местонахождению (почтовому адресу) органа управления юридического лица или лица, имеющего право действовать от имени юридического лица без доверенности;

- предоставления заведомо недостоверных документов или непредставления документов, запрашиваемых в соответствии с законодательством;

- в иных случаях, предусмотренных законодательством.

17. Банку запрещается:

- открывать счета (вклады) на анонимных владельцев, то есть без предоставления открывающим счет (вклад) физическим или юридическим лицом документов, необходимых для его идентификации;

- открывать счета на явно вымышленные имена, не подтвержденные документально;

- открывать счета без личного присутствия лица, открывающего счет, либо его уполномоченного представителя, за исключением случаев, когда Банк имеет возможность провести идентификацию клиента на основании ранее представленных документов, действительных и верифицированных на дату идентификации, а также меры по надлежащей проверке клиентов осуществлены регистрирующим органом либо Банком на основании биометрических данных, а также доверяет результатам надлежащей проверки клиентов, проведенной третьей стороной;

- устанавливать и продолжать отношения с Банками-нерезидентами, не имеющими на территориях государств, в которых они зарегистрированы, физического присутствия и постоянно действующих органов управления;

- выпуск ценных бумаг и других финансовых инструментов на предъявителя;

- осуществлять услуги по получению и отправке денежных средств в иностранной валюте, в том числе через системы международных денежных переводов, без идентификации клиента;

- создавать дочерние Банки, филиалы или представительства на территории государств, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения.

18. При отсутствии возможности осуществить надлежащую проверку клиента, Банк должен рассмотреть вопрос о направлении сообщения об этом в СУГО и отказаться от вступления в деловые отношения или от проведения операции с денежными средствами или иным имуществом такого клиента, либо должен прекратить с ним любые деловые отношения.

§ 1. Физические лица

19. Банк должен располагать достаточным свидетельством идентичности клиента. Документальная проверка личности осуществляется только на основании документов,

которые в соответствии с законодательством Республики Узбекистан являются документами удостоверяющими личность (паспорта или идентификационной ID-карты или заменяющего их документа), или биометрических данных.

20. Идентифицируя физическое лицо, банк должен установить его полное фамилию, имя и отчество, дату и место рождения, гражданство, место постоянного и (или) временного проживания, реквизиты паспорта или идентификационной ID-карты или заменяющего их документа (серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ), идентификационный номер налогоплательщика (если имеется) и номер телефона (домашний/мобильный - если имеется), а также биометрических данных.

21. Информация о клиенте должна быть подтверждена идентификационным документом, удостоверяющим личность (паспорта или идентификационной ID-карты или заменяющего их документа).

Официальный документ:

должен содержать серию и номер, дату выдачи документа, наименование органа, выдавшего документ, фото клиента и другую информацию с целью удостоверения его легальности;

срок действия идентификационного документа должен быть актуальным на момент открытия счета и совершения операций по счету.

Не допускается открытие и закрытие счетов без присутствия самого владельца счета либо его уполномоченного представителя.

На основании биометрических данных должен провести верификацию таких данных с информационной системой Министерства внутренних дел Республики Узбекистан.

22. Документы, удостоверяющие личность (паспорта или идентификационной ID-карты или заменяющего их документа), должны быть представлены в подлинниках, с которых Банк обязан сделать копии и хранить их в соответствующих файлах.

23. При отнесении клиента – физического лица к категории высокого риска, Банк должен применять к такому клиенту усиленные меры по надлежащей проверке, описанные во Внутренних правилах по ПОД/ФТ и ФРОМУ Банка.

§ 2. Юридические лица и индивидуальные предприниматели

24. Банк предпринимает все необходимые меры для получения полного представления о клиенте, его структуре, бенефициарном собственнике, а также получает дополнительную информацию о сфере деятельности клиента и причинах его заинтересованности в том или ином банковском продукте.

25. Банк устанавливает в отношении юридического лица – фирменное наименование, местонахождение (почтовый адрес), а также данные об идентификации физического лица, действующего от имени юридического лица при совершении операции с денежными средствами или иным имуществом. Идентификация юридического лица проводится на основании документов, предоставленных для открытия счета (в т.ч. с единого окна), и иных требуемых в соответствии с законодательством документов. При выполнении мер надлежащей проверки клиентов в отношении юридических лиц Банк должен получить соответствующие документы о государственной регистрации, сведения о руководителях, а также сведения, указанные в учредительных документах.

25-1. Если клиентом или бенефициарным собственником является юридическое лицо, на которое распространяются требования нормативно-правовых актов о раскрытии информации о структуре собственности, то устанавливать и подтверждать личность учредителей (акционеров) такого юридического лица не требуется.

26. Банк в целях более тщательного изучения клиента – юридического лица в процессе надлежащей проверки должен предпринять обоснованные и доступные меры по идентификации физического лица – бенефициарного собственника, которое в конечном итоге является собственником или контролирует клиента, в том числе путем изучения структуры собственности и управления клиента, а также учредителей (акционеров, являющиеся владельцами не менее чем десяти процентов акции общества, участников) клиента.

Банк должен уделять особое внимание:

Составу учредителей клиента, определению лиц, владеющих долей свыше 10% уставного фонда (капитала) клиента;

структуре органов управления клиента и их полномочиям;

размеру зарегистрированного уставного фонда (капитала) клиента.

27. В случае обращения юридических лиц и индивидуальных предпринимателей, учредителями которых являются резиденты Республики Узбекистан, с заявлением о дистанционном открытии банковского счета в процессе прохождения их государственной регистрации, меры по надлежащей проверке клиента, предусмотренные в пункте 26 настоящей Политики, могут быть проведены Центрами государственных услуг (далее — регистрирующий орган) и Банк может доверять результатам проведенных мер. При этом Банк должен удостовериться:

в возможности незамедлительного получения необходимой информации по мерам надлежащей проверки клиента через автоматизированную систему государственной регистрации и постановки на учет субъектов предпринимательства;

в соблюдении требований по проведению мер надлежащей проверки клиентов, установленных в актах законодательства, регистрирующим органом.

В случае невыполнения требований, указанных в абзацах втором и третьем настоящего пункта, Банк самостоятельно проводит меры по надлежащей проверке клиента.

При проведении мер по надлежащей проверке клиентов регистрирующим органом решение о вступлении в деловые отношения с клиентом Банк принимает самостоятельно, исходя от риска. При этом в оферте договора банковского счета должно быть указано возможность проведения мер по надлежащей проверке клиентов Банком.

28. При идентификации юридических лиц Банку необходимо получить также информацию о лицах, которые управляют деятельностью юридического лица, работая в его исполнительных органах, и имеют право распоряжаться его активами и пассивами. При этом в отношении юридических лиц необходимо проверить наименование организации, а также должностных лиц, чьи данные содержатся в карточке с образцами подписей и оттиска печати, с Перечнем.

29. Информация, необходимая при идентификации индивидуальных предпринимателей:

а) информация, предусмотренная для идентификации физических лиц;

б) информация о государственной регистрации: дата, номер, наименование регистрирующего органа;

в) место осуществления деятельности;

г) другие данные, указанные в свидетельстве о государственной регистрации;

д) информация об имеющихся свидетельствах и лицензиях на осуществление видов деятельности: вид деятельности, номер, дата выдачи; кем выдана; срок действия;

е) номера телефонов.

30. При отнесении клиента — юридического лица или индивидуального предпринимателя к категории высокого риска, Банк должен применять к такому клиенту усиленные меры по надлежащей проверке, описанные в Правилах внутреннего контроля по ПОД/ФТ и ФРОМУ АКБ Капиталбанка.

§ 3. Публичные должностные лица

31. Одной из основных задач системы внутреннего контроля Банка является осуществление углубленного мониторинга операций проводимых ПДЛ/ГДЛ/ГС, их близкими родственниками и близкими к ПДЛ/ГДЛ/ГС лицами;

32. Банк помимо применения мер по надлежащей проверке клиента, указанных в настоящих Правилах, в отношении ПДЛ/ГДЛ/ГС, их близких родственников и близких к

ПДЛ/ГДЛ/ГС лицам, выступающих в качестве клиента или бенефициарного собственника клиента, должен:

применять разумные меры для проверки сведений о статусе ПДЛ/ГДЛ/ГС, их близких родственников и близких к ПДЛ/ГДЛ/ГС лиц, и определения источника средств и иного имущества по операции;

устанавливать деловые отношения с ПДЛ/ГДЛ/ГС, их близкими родственниками и близкими к ПДЛ/ГДЛ/ГС лицами, только с разрешения Председателя Правления Банка и его уполномоченного заместителя;

осуществлять постоянный углубленный мониторинг деловых отношений;

33. ПДЛ/ГДЛ/ГС, их близкие родственники, близкие к ПДЛ/ГДЛ/ГС лица относятся к категории высокого уровня риска и Банк должен проявлять к ним повышенное внимание и применять усиленные меры по надлежащей проверке, описанные в Правилах внутреннего контроля по ПОД/ФТ и ФРОМУ АКБ Капиталбанка.

§ 4. Общества и благотворительные учреждения

34. В случае если счета открываются для обществ или благотворительных учреждений Банк должен удостовериться в законности целей создания данных организаций. Банк должен получить всю юридическую документацию таких организаций (в т.ч. с единого окна), персональные данные о бенефициарном собственнике и лицах, уполномоченных для распоряжения счетами. Эти данные должны постоянно обновляться по мере изменения структуры компании и уполномоченных лиц.

§ 5. Кредитные организации

35. При установлении деловых отношений с кредитной организацией, независимо от уровня этих отношений, необходимо в целях идентификации получить и изучить учредительные документы, документы государственной регистрации и иные документы, представленные (в т.ч. с единого окна) для установления деловых отношений. Кроме того, необходимо выяснить, какие меры по противодействию легализации преступных доходов и финансированию терроризма осуществляются данной кредитной организацией.

36. При установлении и осуществлении корреспондентских отношений с Банком – нерезидентом, помимо идентификации данной организации, Банк:

собирает информацию о банке – нерезиденте достаточную для того, чтобы получить полное представление о характере его деловой деятельности;

определяет на основе открытой информации репутацию и качество надзора, в том числе проводились ли в отношении этого банка расследования на предмет легализации доходов, полученных от преступной деятельности и финансирования терроризма;

в отношении «транзитных счетов» - получает удовлетворительное подтверждение того, что банк – корреспондент установил личность и осуществляет проверку клиентов, имеющих прямой доступ к счетам корреспондента и что он имеет возможность предоставить необходимые идентификационные данные о клиенте по запросу банка – корреспондента;

сохранять всю информацию об электронном переводе при установлении отношений с другими Банками в целях осуществления транзитных переводов.

Решение об установлении корреспондентских отношений с банком – нерезидентом принимается Правлением Банка.

37. Банк должен проявлять особое внимание при продолжении корреспондентских отношений с банками-нерезидентами, расположенными на территории государств, не участвующих в международном сотрудничестве в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, или их дочерними банками, филиалами и представительствами.

Банку необходимо убедиться в том, что банки – нерезиденты, с которыми устанавливаются корреспондентские отношения, применяют международные стандарты

проверки и используют соответствующие процедуры проверки к операциям.

38. Банк обязан предпринимать меры, направленные на предотвращение установления отношений с банками - нерезидентами, в отношении которых имеется информация о том,

что их счета используются банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления.

39. При проведении международных расчетов Банк может обмениваться с банками - корреспондентами деталями платежа и другой информацией, связанной с осуществлением международных расчетов.

40. При наличии информации о нарушении банком – нерезидентом требований международных стандартов по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения. Правление Банка должно рассмотреть вопрос о принятии соответствующих мер, вплоть до прекращения сотрудничества с данным банком - корреспондентом.

§ 6. Международные денежные переводы.

41. Банк при установлении и осуществлении отношений с компаниями, предоставляющими услуги по международным денежным переводам, помимо идентификации данной организации:

собирает информацию о партнере по международным денежным переводам для того, чтобы получить полное представление о характере его деловой деятельности;

определяет на основе открытой информации репутацию, в том числе проводились ли в отношении этой организации расследования нарушений, связанных с легализацией доходов, полученных от преступной деятельности, и финансированием терроризма или финансированию распространения оружия массового уничтожения;

сохраняет всю информацию об электронном переводе.

42. Решение об установлении отношений с системами международных денежных переводов, принимается Правлением Банка.

43. Банк при осуществлении операций по международным денежным переводам, в том числе через системы международных денежных переводов, должен:

проводить операции по денежным переводам после надлежащей проверки клиентов - физических лиц;

обеспечить сопровождение отправляемых денежных переводов точными сведениями о клиенте-отправителе;

требовать от банков-нерезидентов и систем международных денежных переводов предоставления минимальной информации об отправителях денежных средств в соответствии с требованиями национального законодательства и внутренних локальных документов Банка;

принимать обоснованные и доступные меры по выявлению международных денежных переводов, не имеющих требуемой информации о получателе и (или) отправителе на основании Порядка об осуществлении мер в АКБ «Капиталбанк» в случаях выявления международных денежных переводов, не имеющих требуемой информации о получателе и (или) об отправителе утвержденного Правлением АКБ Капиталбанк;

уделять особое внимание и проводить тщательный анализ операций, связанных с международными денежными переводами, в которых сведения об отправителе (фамилия, имя, отчество физических лиц, полное наименование юридических лиц, адрес и номер счета отправителя) не представлены либо представлены не в полном объеме.

44. Банк должен иметь возможность получить дополнительную информацию об отправителях денежных средств от корреспондентов банков-нерезидентов и систем международных денежных переводов в соответствии с составленными с ними договорами в течение 3 (трех) банковских дней.

45. В случае отсутствия такой возможности необходимо рассмотреть вопрос расторжения договора с такими системами международных денежных переводов по решению Правления Банка.

46. Если Банк, выступает в качестве посредника (транзитного банка), в платежном переводе, то он должен:

обеспечивать передачу и хранение не менее пяти лет всей информации об отправителе и получателе, сопровождающей электронный перевод, вместе с переводом;

принимать обоснованные и доступные меры по выявлению международных денежных переводов, не имеющих требуемой информации о получателе и (или) отправителе;

рассмотреть вопрос о направлении сообщения в СУГО в случае выявления международных денежных переводов, не имеющих требуемой информации о получателе и (или) отправителе.

§ 7. Валютные операции.

47. Банк взаимодействует с Центральным банком по вопросу предоставления Банку программного комплекса «единой системы обменных пунктов» для регистрации сделок по купле-продаже иностранной валюты с автоматизированной банковской системой.

48. Банк устанавливает банкоматы для оказания услуг по снятию наличной национальной валюты, приобретенной физическими лицами, с международных денежных и банковских переводов, а также оказывает услуги по принятию вкладов в иностранной валюте.

§ 8. Предоставление клиентам банковских услуг.

49. Банк предоставляет клиентам полную информацию об оказываемых Банком услугах, в том числе через размещение данной информации на веб-сайте Банка и информационных стендах филиалов Банка.

50. Банк размещает на собственном веб-сайте программы обучения в виде лекций и видеороликов по услугам и продуктам Банка и механизм получения отдельных видов банковских услуг, а также информации по повышению финансовой грамотности.

51. Разрабатывает и изготавливает необходимые раздаточные материалы по банковским услугам (тарифы, флаера, буклеты).

§ 9. Разработка и внедрение новых видов услуг, технологии и продуктов.

52. Банк должен разрабатывать программу по обеспечения систем дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг и т.д.).

53. Банк разрабатывает механизм по приему и обработке платежных документов клиентов, а также мониторинг состояния платежей и счетов клиентов в круглосуточном режиме через системы дистанционного банковского обслуживания.

54. Банк должен принимать меры по недопущению злоупотребления технологическими достижениями в целях легализации доходов, полученных от преступной деятельности, и финансирования терроризма или финансированию распространения оружия массового уничтожения. В этих целях Банк должен определять и оценивать уровни риска, которые могут возникнуть в связи:

с разработкой новых видов услуг и новой деловой практики;

с использованием новых или развивающихся технологий как для новых, так и для уже существующих видов услуг.

55. Банк должен проводить оценку риска до запуска новых видов услуг, деловой практики или использования новых или развивающихся технологий. При этом определение и оценка данного риска должны осуществляться подразделением Банка, непосредственно внедряющим новые виды услуг (новую технологию), совместно с Департаментом комплаенс контроля.

Данное подразделение банка и Департамент комплаенс контроля должны принимать соответствующие меры для мониторинга и снижения этих рисков.

Информация о результатах осуществленных мер должна предоставляться Правлению Банка.

§ 10. Особые сферы/отрасли бизнеса

56. Банк устанавливает особые сферы бизнеса (включая но не ограничиваясь индустрией игорного бизнеса, криптовалют, развлечений для взрослых, УПДЦ) — взаимодействие с которыми ограничивается или запрещено Правилами внутреннего контроля по ПОД/ФТ и ФРОМУ АКБ Капиталбанка, с ними Банк взаимодействует с осмотрительностью в рамках требований законодательства, риск аппетита, требований партнеров и контрагентов Банка, внутренних порядков и процедур. При установлении деловых отношений Банк проводит изучение деятельности и связей потенциального клиента, корреспондента, агента, или другой третьей стороны на наличие принадлежности к особым сферам бизнеса.

§ 11. Обновление данных о клиентах

57. Банк предпринимает шаги для должного обновления информации о клиентах, полученные в результате надлежащей проверки и идентификации клиента. В целях поддержания информации о клиентах в актуальном состоянии, Банк не реже одного раза в два года обновляет имеющиеся у него сведения о клиентах с низким уровнем риска. Пересмотр и обновление сведений о клиентах с высоким уровнем риска осуществляется не реже одного раза в год. Кроме того, обновление сведений о клиенте может быть осуществлено при совершении клиентом значимых действий (например, возобновление пользования услугами Банка, открытие нового счета), а также при выявлении изменений в органах управления клиента, составе его владельцев и т. д.

ГЛАВА 6. АНАЛИЗ ОПЕРАЦИЙ И МОНИТОРИНГ ДЕЯТЕЛЬНОСТИ КЛИЕНТОВ

58. Основными этапами процедуры мониторинга деятельности клиентов являются: выявление операций и направлений деятельности клиентов, которые требуют дальнейшего изучения;

анализ отчетов о таких операциях ответственным сотрудником Банка;

принятие соответствующих решений о проведении дальнейшего изучения деятельности клиентов по результатам проведенного анализа.

58-1. При этом особое внимание уделяется следующим параметрам:

пользователь счета;

объем и количество операций, проходящих через счет;

источники происхождения средств;

форма, в которой средства были внесены или сняты (наличность, чеки и т.д.);

идентичность лица, проводящего транзакцию;

место направления средств;

свидетельство о целях транзакции;

связей клиента с сотрудниками Банка;

другая необходимая информация в отношении деятельности клиента.

59. В случае обнаружения каких-либо фактов, способствующих, по мнению ответственного сотрудника Банка, в ОД/ФТ и ФРОМУ или у него возникли подозрения касательно легальности операции, Ответственным сотрудником делаются соответствующие записи в виде докладной записки и оповещается руководство Банка.

ГЛАВА 7. ОЦЕНКА УРОВНЯ РИСКА

60. Для определения уровня риска Банк должен принять меры по изучению, анализу, выявлению, оценке, мониторингу, управлению, документированию и снижению уровня риска.

Банк в своей деятельности обязан систематически, не менее одного раза в год проводить изучение, анализ и выявление возможных рисков легализации доходов, полученных от преступной деятельности, финансирования терроризма и финансирования

распространения оружия массового уничтожения, документально фиксировать результаты изучения.

Банк должен определять общий уровень риска, требуемый уровень его снижения и реализовать соответствующую программу мер в зависимости от типов и уровня рисков.

Применяемые меры должны позволять принимать решение о проведении расширенных или упрощенных мер контроля выявленных рисков и эффективном распределении ресурсов.

Уровень риска выявляется и оценивается закрепленными сотрудниками департамента за филиалами на основании представленной клиентом информации с учетом видов деятельности и операций, совершаемых клиентом, критериев, установленных внутренними Правилами, результатов надлежащей проверки клиента, факторов риска (по типам и деятельности клиентов, банковским средствам и услугам, каналам поставок, географическим регионам и другие), в том числе на основании изучения и анализа представленных клиентом информации.

Порядок осуществления мер по изучению, анализу, выявлению, оценке, мониторингу, управлению, документированию и снижению уровня риска устанавливается Правилами внутреннего контроля по ПОД/ФТ и ФРОМУ АКБ Капиталбанка

61. В целях снижения рисков, связанных с вовлечением Банка, а также участия его служащих в осуществлении противоправной деятельности, в том числе легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения, Банк определяет критерии, используемые для оценки риска.

62. На основании полученной в процессе надлежащей проверки клиента информации, с учетом видов деятельности и операций клиента Банк оценивает и присваивает соответствующий (высокий или низкий) уровень риска совершения клиентом операций в целях легализации доходов, полученных от преступной деятельности, или финансирования терроризма или финансированию распространения оружия массового уничтожения.

63. Выявляя и оценивая риски, Банк определяет и использует критерии, принимая во внимание, что основными направлениями оценки являются:

- клиентская база;
- продукты и услуги, предлагаемые Банком;
- географические регионы деятельности Банка.

64. В целях снижения рисков Банк предпринимает следующие меры:

- надлежащая проверка клиентов;
- сбор дополнительной информации о клиентах;
- анализ операций и мониторинг направлений деятельности клиентов.

65. При включении клиента или операции, осуществляемой клиентом, в категорию высокого уровня риска, Банк должен вести постоянный мониторинг за осуществляемыми операциями данного клиента.

66. По мере изменения характера проводимых клиентом операций Банк при необходимости должен пересматривать уровень риска работы с ним. Банк должен уделять повышенное внимание всем сложным, необычно крупным операциям, а также всем необычным схемам совершения операций, не имеющим явной экономической или видимой законной цели.

Результаты оценки рисков в виде отчета должны быть представлены Центральный банк Республики Узбекистан.

ГЛАВА 8. НАПРАВЛЕНИЕ СООБЩЕНИЙ В СУГО

67. После признания операции клиента подозрительной ответственный сотрудник Банка принимает решение о дальнейших действиях Банка в отношении клиента, в том числе: о предоставлении сообщений о подозрительной операции в СУГО;

об извещении соответствующих руководителей Банка (филиала) и подразделений, осуществляющих непосредственную работу с клиентами, о признании операции подозрительной;

- о получении дополнительной информации о клиенте;
- о пересмотре уровня риска работы с клиентом;
- о необходимости особого внимания к проведению операций с клиентом.

68. Ответственный сотрудник Банка вправе внести предложения руководству Банка (филиала) о прекращении договорных отношений с клиентом в соответствии с законодательством и заключенным с ним договором.

69. Сообщение о подозрительной операции передается Банком в СУГО не позднее одного рабочего дня, следующего за днем выявления, в соответствии с порядком, определяемым национальным законодательством.

70. Сообщение в СУГО передается исключительно Головным офисом Банка.

ГЛАВА 9. ХРАНЕНИЕ ИНФОРМАЦИИ И ОТЧЕТНОСТЬ ПО РЕЗУЛЬТАТАМ КОНТРОЛЯ

71. Банк обязан хранить:

информацию и документы, содержащие сведения о клиенте;
сведения об операциях, в том числе информация по которым было направлено сообщение в СУГО;

- отчеты ответственного сотрудника;
- информацию об обучении сотрудников.

72. В целях ограничения доступа к документам (переписка с Центральным банком и СУГО, в том числе бумажные и электронные копии переданных в СУГО сообщений; бумажные и электронные анкеты клиентов; журналы и др.), использованным в деятельности департамента комплаенс контроля (ответственного сотрудника), такие документы и их опись должны храниться непосредственно департаментом комплаенс контроля (ответственным сотрудником) в специально обустроенных помещениях или в несгораемом и опечатываемом сейфе в течение сроков, установленных законодательством, но не менее пяти лет после прекращения деловых отношений с клиентами.

73. Электронные версии документов должны архивироваться программным способом, записываться на электронные носители и храниться директором департамента комплаенс контроля вместе с описью в несгораемом и опечатываемом сейфе.

По истечении сроков хранения, то есть пяти лет документы сдаются в установленном порядке в архив Банка.

74. В целях оценки рисков, связанных с отмыванием доходов, полученных преступным путем, и финансированием терроризма или финансированию распространения оружия массового уничтожения, ответственный сотрудник на ежеквартальной основе представляет отчет председателю Наблюдательного совета и Правления Банка о результатах реализации правил внутреннего контроля в целях противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения.

ГЛАВА 10. ПОРЯДОК ОБУЧЕНИЯ РАБОТНИКОВ БАНКА ПО ВОПРОСАМ ПОД/ФТ и ФРОМУ

75. Банк организует обучение работников вопросам противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения по следующим направлениям на основании плана реализации программы по обучению в АКБ «Капиталбанк» утвержденного Правлением Банка:

- а) ознакомление работников Банка с нормативными и иными актами в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

б) ознакомление работников банка с правилами внутреннего контроля в целях противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, утвержденными Наблюдательным советом банка;

в) обучение и консультирование работников банка по вопросам реализации законодательства Республики Узбекистан в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

76. Программы обучения строятся исходя из того, что основным условием успешного осуществления банком деятельности по противодействию легализации доходов, полученных от преступной деятельности, и финансирования терроризма, является непосредственное участие каждого работника в рамках его компетенции в данном процессе.

77. Целью обучения работников банка является получение ими знаний, необходимых для исполнения требований законодательства Республики Узбекистан в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, а также необходимых для исполнения ими нормативно-правовых актов Республики Узбекистан, Центрального банка в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения и внутренних документов банка по данному направлению.

78. Реализация Порядка осуществляется отчасти путем принятия Плана технической учебы на каждое полугодие в банке. План включает в себя перечень тематику проводимой технической учебы, сроки проведения и фамилии лиц, ответственных за обучения. План утверждается председателем Правления банка не позднее 15 января и 15 июля текущего года. При необходимости в течение года в План могут быть внесены изменения и дополнения, которые утверждаются председателем Правления банка.

79. Сотрудники банка проходят обучение с учетом выполняемых ими функций. Сотрудники, занятые привлечением и обслуживанием клиентов, проведением расчетов, проходят обучение с учетом их функциональных обязанностей. Обучающие программы включают в себя разъяснение необходимости применения процедур надлежащей проверки клиентов, получения дополнительной информации о клиенте и мониторинга его деятельности.

80. Обучение сотрудников вопросам противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма также проводится при переводе на другую работу в рамках банка или при изменении функциональных обязанностей сотрудников.

ГЛАВА 11. ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ

81. Банк ограничивает доступ к информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма или финансированию распространения оружия массового уничтожения, обеспечивают ее нераспространение и не вправе информировать юридических и физических лиц о предоставлении сообщений об их операциях в СУГО.

82. Банк обеспечивает неразглашение (либо использование в личных целях или интересах третьих лиц) ее сотрудниками информации, полученной в процессе выполнения ими функций по внутреннему контролю.

83. Передача информации, в том числе из анкеты, составляющей идентификационные данные клиента, третьим лицам осуществляется в соответствии с законодательством.

84. Настоящая Политика вступает в силу с момента их утверждения Наблюдательным советом АКБ «Капиталбанк».

Внесено:
Директор Департамента
комплаенс контроля



К.А. Хасанов

Согласовано:

Председатель Правления

Заместитель
Председателя Правления

Заместитель
Председателя Правления

Заместитель
Председателя Правления

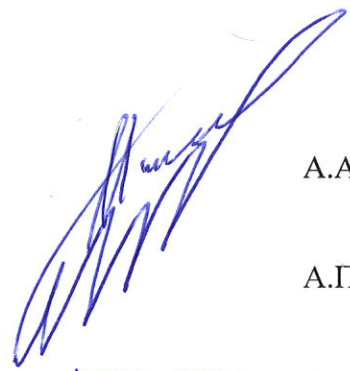
Заместитель
Председателя Правления

Заместитель
Председателя Правления

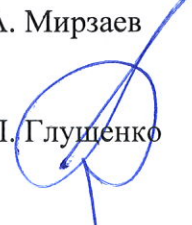
Главный бухгалтер

Директор Департамента
юридической службы

Директор Департамента
по управлению рисками



А.А. Мирзаев

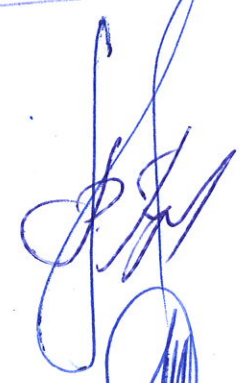


А.П. Глушенко



Б.С.Рахматов

К.В.Тян



Р.Т. Гулямов

С.С. Исмаилов



Д.Н. Аллаёрова



В.В. Пачурин

Т.В. Кан

APPROVED BY
Supervisory Board
"KAPITALBANK" JSCB
Minutes No.48
Dated 27 October, 2022
Signed M.A.Abdusamatov
Chairman, Supervisory Board

**POLICY FOR ANTI-MONEY LAUNDERING,
AND FINANCING OF TERRORISM OR FINANCING OF
PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AT JSCB
"KAPITALBANK"
(New version)**

Tashkent - 2022

PREAMBLE

Taking into account the importance and special significance of the Anti-Money Laundering Policy pursued throughout the civilized world, including taking into account the threat posed to the entire world community by terrorist and related organizations, as well as in order to prevent the threat of money laundering and effective detection and suppression operations aimed at the legalization of criminal proceeds, prevention of intentional or unintentional involvement of the bank in criminal activities and ensuring strict compliance with the requirements of the legislation on combating the legalization of proceeds from crime and the financing of terrorism at JSCB "Kapitalbank" (hereinafter - the bank) a set of measures action aimed at the timely detection of dubious and suspicious transactions has been developed and introduced into operation.

The Bank takes all possible measures to prevent transactions and deals that directly or indirectly relate to the money laundering, as well as to exclude the possibility of conducting transactions related to the financing of terrorist activities or the financing of the proliferation of weapons of mass destruction.

The Bank carefully shall select and build its customer base on the Know Your Customer principle, carefully study its customers, their interests and areas of activity, and seek to establish relationships based on transparency and understanding of customers' business and operations.

CHAPTER 1. GENERAL

1. This Policy on combating money laundering and terrorist financing or proliferation of weapons of mass destruction in "Kapitalbank" JSCB (hereinafter referred to as the Policy) was developed in accordance with the laws of the Republic of Uzbekistan "Regarding Banks and Banking Activities", "Regarding Bank Secrecy", "Regarding combating money laundering and financing of terrorism", as well as the Internal Control Regulations on combating money laundering and financing of terrorism in commercial banks (registered by Ministry of Justice No. 2886 dated 05/23/2017), the Regulation on the minimum requirements for the activities of commercial banks in the implementation of relations with consumers of banking services (registered by the Ministry of Justice No. 3030 dated 07/02/2018), as well as the recommendations of the Group (Intergovernmental Committee) for the development Financial Action Task Force on Money Laundering (FATF).
2. The procedures and regulations specified in this Policy are subject to changes and additions, in accordance with changes in the legislative framework of the Republic of Uzbekistan and international norms and standards.
3. The following basic concepts are used in this Policy:

Internal AML/FT and FPWMD Regulations - Internal Control Regulations on Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction in JSCB "Kapitalbank" (new version);

FATF - Intergovernmental Committee on Combating Money Laundering, which develops world standards in the field of combating money laundering and terrorist financing, and also assesses the compliance of national systems for combating money laundering and terrorist financing with these standards;

Legalization of proceeds from criminal activity means a criminally punishable socially dangerous act, which is giving a legal form to the origin of property (money or other property) by transferring, transforming or exchanging it, as well as concealing or hiding the true nature, source, location, method of disposal, movement, genuine rights in relation to money or other property or its belonging, if money or other property is obtained as a result of criminal activity;

Financing of terrorism means a criminally punishable socially dangerous act aimed at ensuring the existence, functioning, financing of a terrorist organization, traveling abroad or moving through the territory of the Republic of Uzbekistan to participate in terrorist activities, preparing and committing a terrorist act, directly or indirectly providing or collecting any funds, resources, other services to terrorist organizations or persons assisting or participating in terrorist activities;

Financing of proliferation of weapons of mass destruction means provision or collection of any funds, resources, other services for the development, production, acquisition, accumulation, storage, sale, use of nuclear, chemical, biological and other types of weapons of mass destruction, materials and equipment that are known to be used in its creation;

List means a list of persons participating or suspected of participating in terrorist activities or proliferation of weapons of mass destruction, formed by a specially authorized state body on the basis of information provided by state bodies engaged in combating terrorism, proliferation of weapons of mass destruction, and other competent authorities of the Republic of Uzbekistan, and also information received through official channels from the competent authorities of foreign states and international organizations;

Escalation process is the process of transferring the decision to establish business relationships with risk-related Customers or Public officials/Government officials/state agents to senior management or departments that are responsible for AML/FT and FPWMD risks and set appropriate tasks for employees and business;

"Four eyes" principle means the principle stipulating that at least two employees are required to perform the task of internal control. The purpose of the principle is to protect against internal fraud and to prevent sole control. The term is also referred to as "double control", "maker-checker", or "two-crew rule";

Risk is the risk of customers making transactions for the purpose of legalizing proceeds from crime or financing terrorism;

Compliance Control Department of the bank is a structural subdivision of the bank responsible for the implementation of internal control for the purposes of AML /FT and FPWMD and bringing the bank's activities in line with the law requirements;

Responsible Officer is an employee of the bank responsible for the bank's compliance with the rules of internal control for AML/FT and FPWMD and providing information to a specially authorized state body represented by the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan;

Specific Business Areas/Industries means industries/sectors, areas of activity of the Customers (including the industry of gambling, cryptocurrencies, adult entertainment, payment/money service providers, and others), in respect of which the Bank establishes restrictive measures related to the requirements of the law. Interaction with specific areas/branches of business may be acceptable to the Bank subject to the controls established by the customer and/or the Bank;

Gambling (Gambling Business) means a special area/branch of business, games based on risk, providing for a set of actions of its organizers and participants in accordance with a risk-based agreement executed by the organizer of the game (gambling establishment) with one or more participants on winnings, which depends on the chance (event) and (or) abilities, dexterity and other qualities of the participant in the game, including totalizators, casinos, as well as playing with slot machines. Gambling includes businesses with a physical location (for example, casinos, betting shops, and slot machine operators), manufacturers of gaming equipment, remote and online gambling businesses, and providers of gambling software and hosting;

Cryptocurrencies (decentralized virtual currencies) are distributed, open-source, P2P, virtual currencies, a means of digital expression of value that is not issued by a central bank or government agency and is not necessarily pegged to an official currency, which does not have the legal status of a currency or money, but which is accepted as a medium of exchange and can be transferred, stored, bought and sold electronically.

Adult entertainment means any establishment that does not allow minors that sells, rents or displays sexually explicit material or other similar activities;

Money or Value Transfer/Payment Services (MVTs) are services provided by non-banks that include the acceptance of cash, checks, or other means of value and the payment of

the corresponding amount in cash or otherwise to the beneficiary by means of communication, message, transfer or through a clearing house, the network to which the MVTs Provider belongs. Transactions carried out by such services may include one or more intermediaries and final payment to a third party, and may include any new payment methods;

Customer is an individual/legal entity/individual entrepreneur intending to initiate business relations with the bank, or already being serviced by the bank, or carrying out a one-time transaction with the bank on its own behalf in its own interests, or in the interests of third parties;

Participants in the operation are customers, their representatives, as well as partners / counterparties of the customer participating in the operation;

Third party means organizations carrying out operations with money resources or other property;

Beneficial owner means a person who ultimately owns the property rights or effectively controls the customer, and in whose interests a transaction with funds or other property is performed;

Identification of the customer's beneficial owner means determination by the bank of the legal entity of the owner, including the person controlling the customer by studying the structure of ownership and management on the basis of constituent documents determined by law (Articles and (or) Memorandum of association, Regulations);

Public officials (PO) are persons appointed or elected permanently, temporarily or by special authority, performing organizational and administrative functions in state bodies and authorized to perform legally significant actions, as well as persons exercising these functions of an international organization or in legislative, executive, administrative or judicial body of a foreign state;

Government Official (GO)/State Agent (SA) means a citizen of the Republic of Uzbekistan holding an important position in a state body of the Republic of Uzbekistan, who is entrusted or has been entrusted with significant political functions, for example, heads of state or government, prominent politicians, senior government, judicial or military employees, senior executives of state corporations, prominent figures of political parties;

Close relatives of a PO/GO/SA means individuals who are related to a PO/GO/SA directly (blood relation) or marriage or similar (civil) forms of partnership;

Persons close to PO/GO/SA are individuals who are closely related to PO/GO/SA socially or professionally;

A specially authorized state body (hereinafter - SASB) is the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan;

Branch means branches, Banking Services Centers, Operations Department, COD "Kapitalbank" JSCB.

CHAPTER 2. BASIC PRINCIPLES

4. In order to prevent the bank from being involved in operations related to the money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction, the bank shall be guided by the following basic principles:
 - follow the general approaches set out in this policy when creating and improving the internal control system in order to combat money laundering and financing of terrorism;
 - develop own internal control regulations to combat money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction based on national legislation and this policy;
 - take actions aimed at identifying, assessing and reducing the risks associated with the Bank's involvement in AML/FT and FPWMD schemes in all banking operations,

including foreign exchange transactions, bringing the Bank's services to customers, establishing correspondent relationships, as well as developing and introduction of new types of services, technologies and products.

CHAPTER 3. MAIN OBJECTIVES

5. The main objectives in combating money laundering and financing of terrorism are as follows:
 - a) organization of an effective system of internal control to identify transactions subject to reporting to the SASB in all divisions and branches of the Bank;
 - b) effective detection and suppression of transactions with funds or other property aimed at money laundering and financing terrorism or financing proliferation of weapons of mass destruction;
 - c) prevention of intentional or unintentional involvement of the Bank in criminal activities, penetration of criminal capital into its Authorized fund (capital), as well as penetration of criminal persons into the management of the Bank;
 - d) ensuring strict compliance with the requirements of legislation on combating money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction;
 - e) study of the internal control system of other Banks of the Republic of Uzbekistan and foreign Banks when establishing correspondent relations with them.

CHAPTER 4. RESPONSIBLE BANK EMPLOYEE

6. Given that the Bank carries out various types of operations (settlement, cash, deposit, currency, credit operations, etc.), the heads of structural divisions and the management of branches directly involved in these processes are responsible for the implementation of this policy, and general supervision and control shall be carried out by a responsible officer (who is the director of the Compliance Control Department, who manages the activities of employees assigned to branches), approved by the Supervisory Board and appointed by order of the Chairman of the Management Board of the Bank.
7. Director of the Compliance Control Department is independent in making decisions and performing his duties.

Director of the Compliance Control Department has a "veto power" regarding the establishment of a business relationship with a customer and opening of a bank account, transactions or deals aimed at money laundering and financing of terrorism and proliferation of weapons of mass destruction.
8. A responsible employee must be sufficiently authoritative, correct, honest and fair.
9. Duties of the responsible officer shall include:
 - ensuring that other employees of the Bank are aware of the anti-money laundering policy;
 - carrying out inspections for the implementation of procedures stipulated by the regulations on combating money laundering and financing of terrorism in the Bank and monitoring the elimination of identified violations;
 - keeping records, archiving and preserving relevant information and documentation in relation to transactions affected by the regulations on combating money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction;
 - taking effective measures based on the criteria provided for by the internal regulations on money laundering and financing of terrorism in cases of detection of suspicious transactions;

- establish contacts with authorized bodies to comply with the implementation of legislation on combating money laundering and financing of terrorism in accordance with the requirements of the laws of the Republic of Uzbekistan.

CHAPTER 5. IDENTIFICATION PROCEDURES

10. The main way to effectively prevent money laundering is customer due diligence. Customer due diligence is carried out on the basis of information and documents provided by the Bank's customers and includes the "four eyes" principle (verification by two employees) regarding the identification of customer documents and other customer due diligence information.

The escalation process (terms, frequency, step-by-step instructions, responsible persons, etc.) for conducting customer due diligence is regulated by local acts for servicing individuals and legal entities.

11. The Bank shall independently take measures for customers due diligence in the following cases:
 - a) when establishing business and civil law relations, including: when a legal or natural person applies for opening a bank account (deposit);
 - when an individual applies for a bank card;
 - when legal entities and (or) individuals apply for the purchase of securities issued by a commercial Bank;
 - when legal entities and (or) individuals own shares of a commercial Bank, for an amount equal to or greater than one percent of its Authorized capital;
 - when an individual applies for a loan or a service for storing valuables in a bank deposit box;
 - b) when carrying out one-time transactions, including through the performance of one or more transactions related to each other, in the following cases:
 - receipt by customers from the bank cash desk of foreign currency in cash on bank cards issued by other Banks, in an amount equal to or exceeding 100 times the size of the Reference Calculation Value;
 - purchases by individuals of foreign currency in an amount exceeding 100 US dollars in equivalent;
 - carrying out a transaction without opening or using a bank account for an amount equal to or greater than 500 times the Reference Calculation Value;
 - when making or receiving money transfers provided for in paragraph one of clause 34-1, Internal Control Regulations of Kapital Bank JSCB;
 - c) if there are suspicions of money laundering and financing of terrorism, regardless of any exceptions established by the Internal Control Regulations of Kapitalbank JSCB;
 - d) if there are doubts about the reliability or sufficiency of previously obtained data about the customer
12. Customer due diligence measures taken by the Bank are carried out in accordance with the internal AML/FT and FPWMD regulations of the Bank and must include:
 - a) verification of the identity and authority of the customer and the persons on whose behalf it acts on the basis of relevant documents;
 - b) identification of the beneficial owner of the customer;
 - c) study the purpose and nature of the business relationship or planned transactions;
 - d) verifying the accuracy and updating of information about the customer, persons acting on behalf of the customer and the beneficial owner;
 - e) carry out on an ongoing basis the study of business relations and transactions carried out by the customer in order to verify its compliance with information about such a customer and its activities.

In addition to applying the above customer due diligence measures, in relation to a PO/GO/SA acting as a customer or beneficial owner of a customer, the Bank must:

- take reasonable steps to verify the status of PO/GO/SA and to determine the source of funds or other assets of transaction;
- enter into business relations with PO only with the permission of the Chairman of the Management Board of the Bank or his Authorized Deputy;
- carry out continuous in-depth monitoring of business relations.

13. The Bank may trust to the results of customer due diligence carried out by third parties, according to the due diligence measures specified in paragraphs a) and c) – Clause 12 of this Policy. In such cases, the ultimate responsibility for customer due diligence rests with the Bank itself. In doing so, the Bank must ensure:

- possibility of immediate receipt (by means of electronic systems) of the necessary information on customer due diligence;
- possibility, upon request, of immediately obtaining copies of identification data and other relevant customer due diligence documents;
- that third parties are guided by internal regulation on money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction.

In case of non-compliance with one of the requirements provided for in paragraphs two and four of this clause, the Bank shall independently take measures for due diligence of customers.

The Bank decides on entering into a business relationship with a customer on its own, based on the risk, and is entitled to take due diligence measures.

The bank must stipulate the possibility of taking measures for due diligence of customers in the agreement and (or) in the offer agreement.

14. All documents allowing to identify the customer and other participants in the transaction must be valid on the date of its presentation. Documents executed in a foreign language (in whole or in part) shall be submitted to the Bank with a duly certified translation into the state or Russian language, and, if necessary, legalized.

15. The bank, if there are suspicions about the reliability of the information and documents received, must take measures to check (verify) this information and these documents. In this case, the Bank has the right to apply to the relevant organizations with a request to clarify the reliability (authenticity) of information and documents about customers. In addition, the Bank has the right to require the submission of original documents for review, in case of doubts about the reliability of the submitted copies of documents.

16. The Bank has the right to refuse a customer to carry out a transaction with cash or other property in the event of:

- absence at its location (postal address) of a management body of a legal entity or a person entitled to act on behalf of a legal entity without a power of attorney;
- provision of knowingly unreliable documents or failure to provide documents requested in accordance with the law;
- other cases stipulated by the legislation.

17. The Bank shall not:

- open accounts (deposits) for anonymous owners, that is, without providing the individuals or legal entities that open the account (deposit) with the documents necessary for its identification;
- open accounts in clearly fictitious names that are not documented;
- open accounts without the personal presence of the person opening the account or his authorized representative, unless the Bank is able to identify the customer on the basis of previously submitted documents that are valid and verified on the date of identification, as well as customer due diligence measures have been taken by the

registration authority, or Bank on the basis of biometric data, and also trusts the results of customer due diligence conducted by a third party;

- establish and continue relations with non-resident banks that do not have a physical presence and permanent management bodies in the territories of the states in which they are registered;
- issue of securities and other financial instruments to bearer;
- provide services for receiving and sending funds in foreign currency, including through international money transfer systems, without identifying the customer;
- create subsidiaries, branches or representative offices on the territory of states that do not participate in international cooperation in the field of combating money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction.

18. If it is not possible to carry out customer due diligence, the Bank must consider sending a report about this to the SASB and refuse to enter into a business relationship or conduct a transaction with funds or other property of such a customer, or must terminate any business relationship with him.

§ 1 Individuals

19. The Bank must have sufficient proof of the customer's identity. Documentary verification of identity is carried out only on the basis of documents that, in accordance with the legislation of the Republic of Uzbekistan, are identity documents (passport or identification ID-card or a document replacing it), or biometric data.
20. When identifying an individual, the Bank must establish his/her full surname, first name and patronymic, date and place of birth, citizenship, place of permanent and (or) temporary residence, details of the passport or identification ID-card or a document replacing it (series and number of the document, date of issue of the document, name of the authority that issued the document), taxpayer identification number (if available) and telephone number (home / mobile - if available), as well as biometric data.
21. Information about the customer must be confirmed by an identification document proving the identity (passport or identification ID-card or a document replacing it).

Official document:

- must contain the series and number, the date of issue of the document, the name of the authority that issued the document, a photo of the customer and other information in order to certify its legality;
- validity period of the identification document must be current at the time of opening the account and making transactions on the account.

It is not allowed to open and close accounts without the presence of the account holder or his authorized representative.

Based on biometric data, it must verify such data with the information system of the Ministry of Internal Affairs of the Republic of Uzbekistan.

22. Identity documents (passport or ID-card or equivalent document) must be presented in originals, from which the Bank shall make copies and store it in appropriate files.
23. When classifying an individual customer as a high-risk category, the Bank must apply enhanced due diligence measures to such customer, as described in the Bank's Internal AML/FT and FPWMD Regulations.

§ 2 Legal entities and individual entrepreneurs

24. The Bank shall take all necessary measures to obtain a complete picture of the customer, its structure, beneficial owner, and receive additional information about the customer's field of activity and the reasons for its interest in a particular banking product.
25. In relation to a legal entity, the Bank shall establish a company name, location (postal address), as well as data on the identification of an individual acting on behalf of a legal entity when making a transaction with cash or other property. Identification of a legal entity

is carried out based on the documents provided for opening an account (including from a single window), and other documents required in accordance with the law. When performing customer due diligence measures in relation to legal entities, the Bank must obtain the relevant documents on state registration, information about managers, as well as information specified in the constituent documents.

- 25-1. If the customer or beneficial owner is a legal entity that is subject to the requirements of regulatory legal acts on the disclosure of information on the structure of ownership, then it is not required to establish and confirm the identity of the founders (shareholders) of such a legal entity.
26. For the purpose of a more thorough examination of the customer - a legal entity during the due diligence process, the Bank must take reasonable and accessible measures to identify the natural person - beneficial owner, who ultimately owns or controls the customer, including by examining the ownership and management structure of the customer, as well as the founders (shareholders who own at least ten percent of the shares of the company, shareholders) of the customer.

The bank should pay particular attention to:

- composition of founders of the customer, definition of persons owning shares of more than 10% of the Authorized fund (capital) of the customer;
 - structure of the customer's management bodies and their powers;
 - size of the registered authorized fund (capital) of the customer.
27. In the event that legal entities and individual entrepreneurs, whose founders are residents of the Republic of Uzbekistan, apply for remote opening of a bank account in the process of their state registration, the measures for customer due diligence provided for in clause 26 of this Policy may be carried out by the Centers of State services (hereinafter referred to as the registering authority) and the Bank can trust the results of the measures taken. In doing so, the Bank must make certain of:
- the possibility of immediately obtaining the necessary information on the measures of customer due diligence through the automated system of state registration and registration of business entities;
 - compliance with the requirements for conducting customer due diligence measures established in legislative acts by the registering authority.

In case of non-compliance with the requirements specified in paragraphs two and three of this clause, the Bank shall independently take measures for due customer diligence.

When carrying out customer due diligence measures by the registration authority, the Bank makes its own decision to enter into business relations with a customer, based on the risk. At the same time, the offer of the bank account agreement must specify the possibility of carrying out measures for the customer due diligence by the Bank.

28. When identifying legal entities, the Bank must also obtain information about the persons who manage the activities of the legal entity, working in its executive bodies, and have the right to dispose of its assets and liabilities. At the same time, in relation to legal entities, it is necessary to check the name of the organization, as well as officials, whose data are contained in the card with samples of signatures and seal imprints, against the List.
29. Information required for the identification of individual entrepreneurs:
- a) information provided for the identification of individuals;
 - b) information on state registration: date, number, name of the registering authority;
 - c) place of business;
 - d) other data specified in the certificate of state registration;
 - e) information on available certificates and licenses for activities: type of activity, number, date of issue; issued by whom; validity;
 - f) telephone numbers.

30. When classifying a customer - a legal entity or an individual entrepreneur as a high risk category, the Bank must apply to such a customer enhanced due diligence measures described in the Internal Control Regulations for AML/FT and FPWMD of JSCB Kapitalbank.

§ 3. Public officials

31. One of the main objectives of the Bank's internal control system is to carry out in-depth monitoring of transactions conducted by PO/GO/SA, their close relatives and persons close to PO/GO/SA;
32. The Bank, in addition to applying the customer due diligence measures specified in these regulations, in relation to PO/GO/SA, their close relatives and persons close to PO/GO/SA acting as a customer or beneficial owner of a customer, must:
- take reasonable measures to verify information about the status of PO/GO/SA, their close relatives and persons close to PO/GO/SA, and to determine the source of funds and other assets of the operation;
 - establish business relations with PO/GO/SA, their close relatives and persons close to PO/GO/SA only with the permission of the Chairman of the Management Board of the Bank and his Authorized Deputy;
 - carry out continuous in-depth monitoring of business relations;
33. PO/GO/SA, their close relatives, persons close to PO/GO/SA are classified as high-risk and the Bank should pay close attention to them and apply enhanced due diligence measures as described in the Internal Control Regulations on AML/FT and FPWMD of Kapitalbank JSCB.

§ 4. Companies and charitable institutions

34. If accounts are opened for companies or charitable institutions, the Bank must verify the legitimacy of the purpose of creating these organizations. The bank must obtain all legal documentation of such organizations (including from a single window), personal data on the beneficial owner and persons authorized to manage accounts. This data must be constantly updated as the structure of the company and authorized persons change.

§ 5. Credit organizations

35. When establishing business relations with a credit institution, regardless of the level of these relations, it is necessary for identification purposes to obtain and study the constituent documents, state registration documents and other documents submitted (including from a single window) for establishing business relations. In addition, it is necessary to find out what measures are being taken by this credit institution to counteract money laundering and the financing of terrorism.
36. When establishing and implementing correspondent relations with a non-resident Bank, in addition to identifying this organization, the Bank shall:
- collect information about a non-resident bank sufficient to get a complete picture of the nature of its business activities;
 - determine, based on the open information, reputation and quality of supervision, including whether investigations have been carried out against this bank regarding money laundering and financing of terrorism;
 - in respect of "transit accounts", receive satisfactory confirmation that the correspondent bank has identified and verifies the customers with direct access to the correspondent's accounts and that it is able to provide the necessary customer identification data at the request of the correspondent bank;
 - keep all information about the electronic transfer when establishing relations with other Banks for the purpose of making transit transfers.

The decision to establish correspondent relations with a non-resident bank shall be taken by the Management Board of the Bank.

37. The Bank should pay special attention to the continuation of correspondent relations with non-resident banks located in the territory of states that do not participate in international

cooperation in the field of combating money laundering and financing of terrorism, or by their subsidiaries, branches and representative offices.

The bank needs to ensure that non-resident banks with which it establishes correspondent relationships apply international due diligence standards and apply appropriate due diligence procedures to transactions.

38. The bank shall take measures aimed at preventing the establishment of relations with non-resident banks, in respect of which there is information that their accounts are used by banks that do not have permanent management bodies in the territories of the states in which they are registered.
39. When making international settlements, the Bank may exchange with correspondent banks payment details and other information related to the implementation of international settlements.
40. If there is information about a violation by a non-resident bank of the requirements of international standards on combating money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction. The Management Board of the Bank should consider the issue of taking appropriate measures, up to the termination of cooperation with this correspondent bank.

§ 6. International money transfers.

41. When establishing and implementing relations with companies providing services for international money transfers, the Bank, in addition to identifying this organization shall:
 - collect information about the international money transfer partner in order to get a complete picture of the nature of its business activities;
 - determine, based on the open information, reputation, including whether investigations have been carried out against this organization for violations related to money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction;
 - save all information about the electronic transfer.
42. The decision to establish relations with international money transfer systems is made by the Management Board of the Bank.
43. When carrying out operations on international money transfers, including through international money transfer systems, the Bank must:
 - conduct money transfer operations after due diligence of individual customers;
 - ensure that money transfers are accompanied by accurate information about the sending customer;
 - require non-resident banks and international money transfer systems to provide minimum information about the senders of funds in accordance with the requirements of national legislation and internal local documents of the Bank;
 - take reasonable and affordable measures to identify international money transfers that do not have the required information about the recipient and (or) sender on the basis of the Procedure for the implementation of measures in JSCB "Kapitalbank" in cases of identifying international money transfers that do not have the required information about the recipient and (or) on the sender, approved by the Management Board, JSCB Kapitalbank;
 - pay special attention and conduct a thorough analysis of transactions related to international money transfers in which information about the sender (last name, first name, patronymic of individuals, full name of legal entities, address and account number of the sender) is not provided or is not provided in full.
44. The bank must be able to obtain additional information about senders of funds from correspondents of non-resident banks and international money transfer systems in accordance with the agreements drawn up with them within 3 (three) banking days.

45. In the absence of such an opportunity, it is necessary to consider the issue of terminating the agreement with such systems of international money transfers by decision of the Board of the Bank.
46. If the Bank acts as an intermediary (transit bank) in the payment transfer, then it must:
- ensure the transfer and storage of all information about the sender and recipient accompanying the electronic transfer, together with the transfer, for at least five years;
 - take reasonable and affordable measures to identify international money transfers that do not have the required information about the recipient and (or) sender;
 - consider the issue of sending a message to the SASB in case of detection of international money transfers that do not have the required information about the recipient and (or) the sender.

§ 7 Currency transactions.

47. The Bank shall interact with the Central Bank on the issue of providing the Bank with a software package of the "unified system of exchange offices" for registering transactions for the purchase and sale of foreign currency with an automated banking system.
48. The Bank shall install ATMs to provide services for withdrawing cash in national currency purchased by individuals from international money and bank transfers, and also provide services for accepting deposits in foreign currency.

§ 8 Provision of banking services to customers.

49. The Bank shall provide customers with complete information about the services provided by the Bank, including by posting this information on the Bank's website and information stands of the Bank's branches.
50. The Bank shall place on its website training programs in the form of lectures and videos on the services and products of the Bank and the mechanism for obtaining certain types of banking services, as well as information on improving financial literacy.
51. The Bank shall develop and produce the necessary distribution materials for banking services (tariffs, flyers, booklets).

§ 9 Development and implementation of new types of services, technologies and products.

52. The bank should develop a program to provide remote banking systems (Internet banking, mobile banking, etc.).
53. The Bank is developing a mechanism for receiving and processing customer payment documents, as well as monitoring the status of payments and customer accounts within 24 hours through remote banking systems.
54. The Bank should take steps to ensure that technological advances are not misused for the purpose of money laundering and financing terrorism or financing proliferation of weapons of mass destruction. To this end, the Bank must determine and evaluate the levels of risk that may arise in connection with:
- development of new types of services and new business practices;
 - using new or developing technologies for both new and existing services.
55. The bank should conduct a risk assessment before launching new services, business practices, or using new or developing technologies. At the same time, the definition and assessment of this risk should be carried out by the Bank's division directly implementing new types of services (new technology), together with the Compliance Control Department.

This division of the bank and the Compliance Control Department must take appropriate measures to monitor and mitigate these risks.

Information on the results of the measures taken must be provided to the Management Board of the Bank.

§ 10. Special areas / branches of business

56. The Bank shall establish special areas of business (including but not limited to the industry of gambling, cryptocurrencies, adult entertainment, MVTs) - interaction with which is limited or prohibited by the Internal Control Regulations on AML/FT and FPWMD of Kapitalbank JSCB, with which the Bank interacts with discretion in within the framework of legal requirements, the risk of appetite, the requirements of partners and counterparties of the Bank, internal procedures and procedures. When establishing a business relationship, the Bank shall examine the activities and relationships of a potential customer, correspondent, agent, or other third party for the presence of belonging to specific areas of business.

§ 11. Updating customer data

57. The Bank shall take steps to properly update customer information obtained as a result of customer due diligence and identification. In order to keep information about customers up to date, the Bank shall update the information it has about low-risk customers at least once every two years. High-risk customer information shall be reviewed and updated at least once a year. In addition, information about the customer can be updated when the customer performs significant actions (for example, resuming use of the Bank's services, opening a new account), as well as when changes are detected in the customer's management bodies, the composition of its owners, etc.

CHAPTER 6. ANALYSIS OF OPERATIONS AND MONITORING OF CUSTOMERS PERFORMANCE

58. The main stages of the procedure for monitoring the customers activities are as follows:
- identification of operations and activities of customers that require further study;
 - analysis of reports on such transactions by a responsible employee of the Bank;
 - making appropriate decisions on conducting further study of the activities of customers based on the results of the analysis.
- 58-1. In this case, special attention shall be paid to the following parameters:
- account user;
 - volume and number of transactions passing through the account;
 - sources of origin of funds;
 - form in which the funds are deposited or withdrawn (cash, checks, etc.);
 - identity of the person conducting the transaction;
 - place of funds transfer;
 - evidence of the purpose of transaction;
 - relations of the customer with employees of the Bank;
 - other necessary information regarding activities of the customer.
59. If any facts are discovered that, in the opinion of the responsible officer of the Bank, contribute to AML/FT and FPWMD or he has suspicions about the legality of the operation, the Responsible officer shall make appropriate entries in the form of a memorandum and notify the management of the Bank.

CHAPTER 7. RISK ASSESSMENT

60. To determine the level of risk, the Bank must take measures to study, analyze, identify, evaluate, monitor, manage, document and reduce the level of risk.
- The Bank in its activities shall systematically, at least once a year, study, analyze and identify possible risks of money laundering, financing of terrorism and financing proliferation of weapons of mass destruction, and document the results of the study.
- The bank must determine the overall level of risk, the required level of its reduction and implement an appropriate program of measures depending on the types and level of risks.
- The measures applied should allow decisions to be made on the implementation of enhanced or simplified measures to control the identified risks and the effective allocation of resources.

The level of risk shall be identified and assessed by the employees of the department assigned to the branches based on the information provided by the customer, taking into account the types of activities and transactions performed by the customer, the criteria established by internal Regulations, the results of customer due diligence, risk factors (by types and activities of customers, banking facilities and services, supply channels, geographic regions, etc.), including on the basis of the study and analysis of information provided by the customer.

The procedure for taking measures to study, analyze, identify, evaluate, monitor, manage, document and reduce the level of risk shall be established by the Internal Control Regulations for AML/FT and FPWMD of Kapitalbank JSCB.

61. In order to reduce the risks associated with the involvement of the Bank, as well as the participation of its employees in the implementation of illegal activities, including money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction, the Bank shall determine the criteria used to assess risk.
62. Based on the information obtained in the process of customer due diligence, taking into account the types of activities and operations of the customer, the Bank shall assess and assign an appropriate (high or low) risk level to the customer to perform operations for the purpose of money laundering, or financing terrorism or financing proliferation weapons of mass destruction.
63. When identifying and assessing risks, the Bank shall determine and use criteria, taking into account that the main areas of assessment are:
 - customer base;
 - products and services offered by the Bank;
 - geographical regions of the Bank's operations.
64. In order to reduce risks, the Bank shall take the following measures:
 - customer due diligence;
 - collecting additional information about customers;
 - analysis of operations and monitoring of customer activities.
65. When a customer or a transaction carried out by a customer is included in the high-risk category, the Bank must constantly monitor the transactions carried out by this customer.
66. As the nature of the operations carried out by the customer changes, the Bank, if necessary, must review the level of risk of working with him. The Bank should pay close attention to all complex, unusually major transactions, as well as all unusual patterns of transactions that do not have a clear economic or apparent legal purpose.

The results of the risk assessment in the form of a report must be submitted to the Central Bank of the Republic of Uzbekistan.

CHAPTER 8. DIRECTING MESSAGES TO SASB

67. After the customer's transaction is recognized as suspicious, the responsible officer of the Bank shall decide on further actions of the Bank in relation to the customer, including:
 - provision of reports of suspicious transactions in the SUGO;
 - notifying the relevant managers of the Bank (branch) and departments that work directly with customers about the recognition of the operation as suspicious;
 - obtaining additional information about the customer;
 - reviewing the level of risk of working with a customer;
 - the need for special attention to the conduct of transactions with the customer.
68. The responsible employee of the Bank has the right to make proposals to the management of the Bank (branch) on the termination of contractual relations with the customer in accordance with the law and the agreement concluded with it.

69. A report on a suspicious transaction shall be submitted by the Bank to the SASB no later than one business day following the day of detection, in accordance with the procedure determined by national legislation.
70. A message to the SASB shall be transmitted exclusively by the Head Office of the Bank.

CHAPTER 9. RETENTION OF INFORMATION AND REPORTING ON CONTROL RESULTS

71. The Bank shall keep:
- information and documents containing information about the customer;
 - information about transactions, including information on which a message is sent to the SASB;
 - reports of the responsible officer;
 - information about employee training.
72. In order to limit access to documents (correspondence with the Central Bank and the SASB, including paper and electronic copies of messages sent to the SASB; paper and electronic customer profiles; magazines, etc.) used in the activities of the Compliance Control Department (responsible officer) , such documents and its inventory must be stored directly by the Compliance Control Department (responsible officer) in specially equipped premises or in a fireproof and sealed safe for the periods established by law, but not less than five years after the termination of business relations with customers.
73. Electronic versions of documents must be archived programmatically, recorded on electronic media and stored by the Director of the Compliance Control Department together with the inventory in a fireproof and sealed safe.
- After the expiration of the storage period, that is, five years, the documents shall be submitted in the prescribed manner to the Bank's archive.
74. In order to assess the risks associated with money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction, the responsible officer shall on a quarterly basis submit a report to the Chairman of the Supervisory Board and the Management Board of the Bank on the results of implementation of internal control regulations in order to combat money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction.

CHAPTER 10. PROCEDURE FOR TRAINING THE BANK'S EMPLOYEES ON AML/FT AND FPWMD ISSUES

75. The Bank shall organize training of employees on money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction in the following areas on the basis of the plan for implementation of the training program at JSCB "Kapitalbank" approved by the Management Board of the Bank:
- a) familiarization of the Bank's employees with regulations and other acts in the field of money laundering and financing of terrorism;
 - b) familiarization of the bank's employees with the regulations of internal control in order to combat money laundering and financing of terrorism, approved by the Supervisory Board of the Bank;
 - c) training and advising bank employees on the implementation of the legislation of the Republic of Uzbekistan in the field of combating money laundering and financing of terrorism.
76. Training programs shall be based on the fact that the main condition for the successful implementation by the bank of activities to combat money laundering and financing of terrorism is the direct participation of each employee within its competence in this process.
77. The purpose of training bank employees is to obtain the knowledge necessary for them to comply with the requirements of the legislation of the Republic of Uzbekistan in the field of combating money laundering and financing of terrorism, as well as regulatory legal acts of the Republic of Uzbekistan, the Central Bank in the field of combating money laundering

and financing of terrorism or financing of proliferation of weapons of mass destruction and internal documents of the bank in this area.

78. The implementation of the Policy shall be carried out in part through the adoption of a Technical Study Plan for each half year in the bank. The plan shall include a list of topics of ongoing technical training, dates and names of persons responsible for the training. The plan shall be approved by the Chairman of the Management Board of the bank no later than January 15 and July 15 of the current year. If necessary, changes and additions may be made to the Plan during the year, which shall be approved by the Chairman of the Board of the Bank.
79. Bank employees shall be trained taking into account the functions they perform. Employees involved in attracting and servicing customers, making settlements, shall be trained taking into account their functional duties. The training programs shall include explaining the need for customer due diligence procedures, obtaining additional information about the customer and monitoring its activities.
80. Training of employees on issues of combating money laundering and financing of terrorism shall be also carried out when transferring to another job within the bank or when changing the functional duties of employees.

CHAPTER 11. CONFIDENTIALITY

81. The Bank shall restrict access to information related to combating money laundering and financing of terrorism or financing of proliferation of weapons of mass destruction, ensure its non-proliferation and shall not inform legal entities and individuals about the provision of reports on their operations to SASB.
82. The Bank shall ensure non-disclosure (or use for personal purposes or interests of third parties) by its employees of information obtained in the course of their performance of internal control functions.
83. The transfer of information, including from the questionnaire constituting the customer's identification data, to third parties shall be made in accordance with the law.
84. This Policy shall enter into force upon its approval by the Supervisory Board of JSCB "Kapitalbank".

Proposed by:

Director, Compliance Control Department: signed K.A. Khasanov

Agreed by:

Chairman, Management Board:	signed	A.A.Mirzaev
Deputy Chairman, Management Board:	signed	A.P.Glushchenko
Deputy Chairman, Management Board:	signed	B.S. Rakhmanov
Deputy Chairman, Management Board:	signed	K.V.Tyan
Deputy Chairman, Management Board:	signed	R.T. Gulyamov
Deputy Chairman, Management Board:	signed	S.S. Ismailov
Chief Accountant:	signed	D.N. Allayorova
Director, Legal Services Department:	signed	V.V. Pachurin
Director, Risk Management Department:-	signed	T.V. Kan

Республика Узбекистан. Город Ташкент.

Перевод выполнен переводчиком **Нурматовой Санобар Шухрат кизи**. Паспорт АА №0823182, выданный 07.02.2013 г. Сергелийским РОВД.

Перевод данного текста полностью соответствует тексту оригинала, я **Нурматова Санобар Шухрат кизи**, владелец диплома **В № 570006**, выданного Узбекским Государственным Университетом Мировых Языков, от 08 июня 2011 года, удостоверяю правильность перевода с узбекского и русского языков на английский язык текста записей и печати в изложенном документе. Об ответственности за ложный и неверный перевод предупреждена нотариусом.

Переводчик не несет ответственности за содержание и достоверность информации в изложенном оригинале документа.

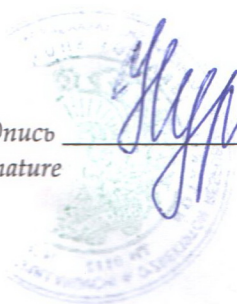
Republic of Uzbekistan. Tashkent City.

The translation was made by translator **Nurmatova Sanobar Shukhrat kizi**, passport details: AA#0823182, issued by Department of Internal Affairs of Sergeli district.

Translation of the text completely corresponds to the original text. I **Nurmatova Sanobar Shukhrat kizi**, holder of **Diploma: B № 570006**, issued on June 8, 2011 by Uzbek State University of World Languages, certify to the accuracy of the translation from Uzbek and Russian languages into English of the text and seals set out in this document. I am warned of responsibility for false and incorrect translation by Notary.

The translator is not responsible for the content of the original document.

Подпись
Signature



Нурматова С.Ш.

За дополнительной информацией обращайтесь по тел: +998 90 374 06 68

For more information please dial: : +998 90 374 06 68

19 ДЕК 2022

Я, Исраилов Шухрат Келдиёрович, нотариус нотариальной конторы Яккасарайского района города Ташкента занимающийся частной практикой, лицензия TN №0112 выдана Управлением юстиции города Ташкента от 28.04.2020 года, свидетельствую подлинность подписи известного мне переводчика Нурматовой Санобар Шухрат кизи. Личность подписавшего документа установлена, дееспособность проверена, т.е. при личном общении с ней, её дееспособность сомнений не вызвала.

Мною, лицу, обратившемуся за совершением нотариального действия, разъяснено, что при свидетельствовании верности подлинности подписи не подтверждается законность содержания документа, и соответствие изложенных в нём фактов действительности, а лишь подтверждается, что подпись сделана определённым лицом.

На основании статьи 67 «Закона о нотариате» Республики Узбекистан, нотариус, свидетельствуя подлинность подписи, не удостоверяет факты, изложенные в документе, а лишь подтверждает, что подпись сделана определённым лицом.

Зарегистрировано в электронном реестре за № 20220194203 0343.

Взыскано государственной пошлины 15 000 сум.

(Пятнадцать тысяч сум)

Нотариус



Исраилов Ш.К.



Republic of Uzbekistan. Tashkent city



I, Israilov Shukhrat Keldiyorovich, Notary of Yakkasaray district, Tashkent city, carrying out private activity, license TN No.0112 issued on 28.04.2020 by the Department of Justice of Tashkent city, hereby certify the authenticity of signature made by translator Nurmatova Sanobar Shukhrat kizi. The personality of signed person is established. The personality of person, who signed this document, was established her capability was proved, i.e. at dialogue with her any doubts did not call.

It is explained by me to applying person for notarial action, that in certifying fidelity of authenticity of signature, the legality of document's content and compliance of facts set out herein is not confirmed, but only certifies that the signature was made by a certain person.

According to article 67 of the Law about Notariat, the notary, certifying authenticity of the signature, does not certify the facts stated in the document, and only confirms the signature is made by the certain person.

Registered under electronic registry No. 20220194202

State Duty UZS 15 000 UZS

(Fifteen thousand UZS)

Notary signed

Official Seal of Notary