Алматы қаласы город Алматы

**О внесении изменений и дополнений**

**в некоторые нормативные правовые акты Республики Казахстан**

**по вопросам регулирования банковской деятельности**

Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка **ПОСТАНОВЛЯЕТ**:

1. Утвердить Перечень нормативных правовых актов Республики Казахстан по вопросам регулирования банковской деятельности, в которые вносятся изменения и дополнения, согласно приложению к настоящему постановлению (далее - Перечень).

2. Департаменту методологии и пруденциального регулирования финансовых организаций в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка.

4. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального [опубликования](http://online.zakon.kz/Document/?doc_id=37778124), за исключением абзацев двести пятого и двести шестого пункта 2 Перечня, которые вводятся в действие с 1 сентября 2025 года.

|  |  |  |
| --- | --- | --- |
| **Должность** |  | **ФИО** |

«СОГЛАСОВАНО»

Агентство Республики Казахстан

по финансовому мониторингу

Приложение к постановлению  
Правления Агентства  
Республики Казахстан  
по регулированию и развитию  
финансового рынка  
от \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_

**Перечень нормативных правовых актов Республики Казахстан**

**по вопросам регулирования банковской деятельности,**

**в которые вносятся изменения и дополнения**

1. Внести в [постановление](http://online.zakon.kz/Document/?doc_id=39795745) Правления Национального Банка Республики Казахстан от 29 июня 2018 года № 140 «Об утверждении Требований к надлежащей проверке клиентов в случае дистанционного установления деловых отношений субъектами финансового мониторинга» (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 17250) следующее дополнение:

дополнить пунктом 7-1 следующего содержания:

«7-1. В случае идентификации и аутентификации клиента посредством использования средств биометрической идентификации субъектом финансового мониторинга обеспечивается хранение записи сеанса видеоконференции с клиентом либо полученного текущего изображения клиента с помощью технологии выявления движения не менее пяти лет со дня прекращения деловых отношений с клиентом.».

2. Внести в [постановление](http://online.zakon.kz/Document/?doc_id=35598681) Правления Национального Банка Республики Казахстан от 12 ноября 2019 года № 188 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан» (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 19632) следующие изменения и дополнения:

в Правилах формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан, утвержденных указанным постановлением:

пункт 2 изложить в следующей редакции:

«2. В Правилах используются следующие понятия:

1) риск информационной безопасности - вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов банка;

2) риск информационных технологий - вероятность возникновения ущерба вследствие отказа (нарушения функционирования) информационно-коммуникационных технологий, эксплуатируемых банком;

3) центр обмена данными по платежным транзакциям с признаками мошенничества (далее - антифрод-центр НБРК) - юридическое лицо Национального Банка Республики Казахстан, которое осуществляет меры, направленные на предотвращение платежных транзакций с признаками мошенничества и иных противоправных инцидентов, к которым относятся в рамках настоящих Правил признаки связанности платежных транзакций с незаконным производством, оборотом и (или) транзитом наркотиков, организацией деятельности финансовых пирамид, осуществлением платежей и (или) переводов денег в пользу электронного казино и интернет-казино (далее – иные противоправные инциденты);

4) риск мошенничества и иных противоправных инцидентов - вероятность возникновения финансовых потерь и репутационных рисков, вовлечения банка в противоправные действия вследствие мошенничества со стороны третьих лиц и (или) работников банка, использования финансовых услуг банка в операциях, связанных с незаконным производством, оборотом и (или) транзитом наркотиков, организацией деятельности финансовых пирамид и для осуществления платежей и (или) переводов денег в пользу электронного казино и интернет-казино;

5) антифрод-система банка - комплекс технических и аналитических мер, направленных на предотвращение и обнаружение операций с признаками мошенничества и иных противоправных инцидентов, выявление дропперов при предоставлении банковских услуг;

6) уполномоченный коллегиальный орган банка - совет директоров, комитет при совете директоров, правление, комитет при правлении;

7) репутационный риск - вероятность возникновения потерь, неполучения запланированных доходов в результате сужения клиентской базы, снижения иных показателей развития вследствие формирования в обществе отрицательного представления о надежности банка, качестве оказываемых им услуг или характере деятельности банка в целом;

8) дроппер - лицо, предоставившее третьему лицу доступ к своему банковскому счету и (или) средству электронного платежа, а равно передавшее свои платежные инструменты в пользование третьему лицу, в том числе, за материальное вознаграждение, повлекшее их несанкционированное использование в противоправных операциях;

9) юридический риск - вероятность возникновения потерь вследствие несоблюдения банком либо контрагентом требований гражданского, налогового, банковского законодательства Республики Казахстан, законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, законодательства Республики Казахстан о валютном регулировании и валютном контроле, о платежах и платежных системах, о пенсионном обеспечении, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о кредитных бюро и формировании кредитных историй, о коллекторской деятельности, об обязательном гарантировании депозитов, о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, об акционерных обществах, а в отношениях с нерезидентами Республики Казахстан - законодательства страны его происхождения, а также условий заключенных договоров;

10) внутренний процесс оценки достаточности капитала - набор процессов управления существенными рисками, с учетом объема активов, характера и уровня сложности деятельности, организационной структуры, стратегических планов, риск-профиля банка, нормативной правовой базы, оценка и агрегирование таких рисков с целью определения целевого уровня достаточности капитала банка для поддержания стабильного финансового положения и платежеспособности.

Под капиталом филиала банка-нерезидента Республики Казахстан понимаются активы филиала банка-нерезидента Республики Казахстан, принимаемые в качестве резерва, рассчитанные в соответствии с требованиями постановления Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 12 февраля 2021 года № 23 «Об установлении пруденциальных нормативов и иных обязательных к соблюдению норм и лимитов для филиалов банков-нерезидентов Республики Казахстан (в том числе филиалов исламских банков-нерезидентов Республики Казахстан), их нормативных значений и методики расчетов, включая порядок формирования активов филиалов банков-нерезидентов Республики Казахстан (в том числе филиалов исламских банков-нерезидентов Республики Казахстан), принимаемых в качестве резерва, и их минимальный размер», зарегистрированного в Реестре государственной регистрации нормативных правовых актов под № 22213 (далее - Постановление № 23);

11) план финансирования капитала - совокупность процедур и плана действий для реагирования на критическое снижение капитала банка;

12) статистический журнал стоимости залогового обеспечения - внутренний журнал стоимостей залогового обеспечения, включающий описание и характеристику залогового обеспечения, информацию по итогам первой и наиболее актуальной оценок независимой оценки качества (дата оценки, наименование независимой оценки качества, стоимость, метод оценки), заключения залоговой службы (дата, стоимость), причины различия стоимостей, информацию по реализации (при наличии);

13) беззалоговый потребительский заем - банковский заем без условия о залоге на момент выдачи, предоставленный физическому лицу на цели, не связанные с осуществлением предпринимательской деятельности;

14) комплаенс-риск - вероятность возникновения потерь вследствие несоблюдения банком и его работниками требований гражданского, налогового, банковского законодательства Республики Казахстан, законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, законодательства Республики Казахстан о валютном регулировании и валютном контроле, о платежах и платежных системах, о пенсионном обеспечении, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о кредитных бюро и формировании кредитных историй, о коллекторской деятельности, об обязательном гарантировании депозитов, о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, об акционерных обществах, внутренних документов банка, регламентирующих порядок оказания банком услуг и проведения операций на финансовом рынке, а также законодательства иностранных государств, оказывающего влияние на деятельность банка;

15) корпоративное управление - система взаимоотношений между правлением банка (соответствующим исполнительным органом банка-нерезидента Республики Казахстан, филиал которого открыт на территории Республики Казахстан, руководящими работниками филиала банка-нерезидента Республики Казахстан), советом директоров (соответствующим органом управления банка-нерезидента Республики Казахстан, филиал которого открыт на территории Республики Казахстан) акционерами, руководящими работниками и аудиторами, а также взаимоотношения между уполномоченными коллегиальными органами банка.

Система корпоративного управления позволяет организовать распределение полномочий и ответственности, а также построить процесс принятия корпоративных решений;

16) кредитный риск - вероятность возникновения потерь, возникающая вследствие невыполнения заемщиком или контрагентом своих обязательств в соответствии с условиями договора банковского займа;

17) кредитоспособность - комплексная правовая и финансовая характеристика заемщика, представленная финансовыми и нефинансовыми показателями, позволяющая оценить его возможность в будущем полностью и в срок исполнить обязательства по договору банковского займа;

18) кредитный договор - соглашение между банком и заемщиком о предоставлении финансирования (включая условное финансирование), в результате которого у банка возникают (либо возникнут в будущем) требования к заемщику;

19) план финансирования на случай непредвиденных обстоятельств - совокупность процедур и плана действий для реагирования на снижение способности банка своевременно отвечать по своим обязательствам;

20) надзорное стресс-тестирование — это инструмент уполномоченного органа, направленный на оценку финансовой устойчивости банков к гипотетическим (стрессовым) сценариям развития событий. Банки на основании единой для всех участников надзорного стресс-тестирования методологии и сценариев проводят расчеты с использованием внутренних моделей и предоставляют в уполномоченный орган результаты стресс-тестирования. При этом банки отвечают за надлежащее качество проведенных расчетов и результаты стресс-тестирования;

21) уполномоченный орган по финансовому мониторингу - государственный орган, осуществляющий финансовый мониторинг и принимающий иные меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, финансированию распространения оружия массового уничтожения;

22) подразделение-владелец защищаемой информации - подразделение банка, владелец информации, нарушение конфиденциальности, целостности или доступности которой приведет к убыткам для банка;

23) критичный информационный актив - информационный актив, определяемый в соответствии с постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под   
№ 16772 (далее - Постановление № 48);

24) существенный риск - риск, реализация которого приведет к ухудшению финансовой устойчивости банка;

25) конфликт интересов - ситуация, при которой возникает противоречие между личной заинтересованностью должностных лиц банка (должностных лиц органа управления, исполнительного органа банка-нерезидента Республики Казахстан, филиал которого открыт на территории Республики Казахстан, руководящих работников филиала банка-нерезидента Республики Казахстан), его акционеров и (или) его работников и надлежащим исполнением ими своих должностных полномочий или имущественными и иными интересами банка и (или) его работников и (или) клиентов, которое повлечет за собой неблагоприятные последствия для банка и (или) его клиентов;

26) рыночный риск - вероятность возникновения финансовых потерь по балансовым и внебалансовым статьям, обусловленная неблагоприятными изменениями рыночной ситуации, выражающаяся в изменениях рыночных процентных ставок, курсов иностранных валют, рыночной стоимости финансовых инструментов, товаров;

27) база данных инцидентов - база инцидентов с признаками мошенничества и иных противоправных инцидентов, которая ведется банком в электронном виде;

28) операционный риск - вероятность возникновения потерь в результате неадекватных и недостаточных внутренних процессов, человеческих ресурсов и систем, или влияния внешних событий, за исключением стратегического риска и репутационного риска;

31) внутренний процесс оценки достаточности ликвидности - набор процессов управления риском ликвидности, в целях поддержания банком надлежащего уровня ликвидности и внедрения надлежащей системы управления риском ликвидности в различные временные интервалы в зависимости от видов деятельности, валюты;

32) риск ликвидности - вероятность возникновения финансовых потерь в результате неспособности банка выполнить свои обязательства в установленный срок без значительных убытков;

33) процентный риск - риск возникновения финансовых расходов (убытков) вследствие неблагоприятного изменения процентных ставок по активам, пассивам банка;

34) политика - утвержденный советом директоров банка внутренний документ, определяющий основные количественные и качественные параметры, принципы, стандарты, обеспечивающие эффективное функционирование банка и соответствие его деятельности стратегии, риск-профилю, риск-аппетиту. В рамках политики совет директоров банка обеспечивает наличие соответствующих внутренних документов, описывающие отдельные процедуры, процессы, инструкции;

35) стратегический риск - вероятность возникновения убытков в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегическое развитие банка и выражающихся в недостаточном учете возможных опасностей, присущих деятельности банка, неправильном или недостаточно обоснованном определении перспективных направлений деятельности, в которых банк достигнет преимущества перед конкурентами, отсутствии или обеспечении в неполном объеме необходимых ресурсов и организационных мер, обеспечивающих достижение стратегических целей деятельности банка;

36) стресс-тестирование - метод оценки потенциального влияния исключительных, но возможных событий на финансовое состояние банка;

37) риск - вероятность того, что ожидаемые или непредвиденные события окажут отрицательное влияние на финансовую устойчивость банка, его капитал и (или) доходы;

38) риск-профиль - совокупность видов риска и иных сведений, характеризующих степень подверженности банка рискам, присущим всем видам деятельности банка для выявления слабых сторон и определения приоритетности последующих действий в рамках системы управления рисками;

39) риск-аппетит - агрегированный (агрегированные) уровень (уровни) существенных рисков (лимиты допустимого размера риска), который (которые) банк готов принять либо намерен исключить при реализации стратегии;

40) заявление риск-аппетита - утверждаемый советом директоров банка документ, описывающий агрегированный (агрегированные) уровень (уровни) существенных рисков (лимиты допустимого размера риска), который (которые) банк готов принять либо намерен исключить при реализации стратегии. Заявление риск-аппетита содержит заявление качественного характера, а также количественного характера, включая показатели в отношении доходности, капитала, ликвидности, рисков, иных применимых показателей;

41) риск-культура - процессы, процедуры, внутренние правила банка, направленные на понимание, принятие, управление и контроль за рисками с целью минимизации их влияния на финансовое состояние банка, а также этические нормы и стандарты профессиональной деятельности всех участников организационной структуры. Риск-культура дополняет существующие утвержденные процедуры, процессы и механизмы деятельности банка и является неотъемлемым компонентом системы управления рисками;

42) обработка риска - процесс выбора и реализации мер по изменению рисков;

43) реестр рисков - структурированный перечень рисков, содержащий критерии и причины возникновения рисков, вероятность их возникновения, воздействие (ущерб), приоритет и способы обработки риска;

44) уполномоченный орган - государственный орган, осуществляющий государственное регулирование, контроль и надзор финансового рынка и финансовых организаций;

45) организационная структура - внутренний документ и (или) совокупность внутренних документов, устанавливающих количественный состав и систему органов управления, руководящих работников и структурных подразделений банка, отражающий структуру подчиненности, подотчетности;

46) участник Международного финансового центра «Астана», оказывающий услуги по управлению платформой цифровых активов- юридическое лицо, зарегистрированное в соответствии с действующим правом Международного финансового центра «Астана» и осуществляющее на территории Международного финансового центра «Астана» деятельность по управлению платформой цифровых активов;

47) внутренний (экономический) капитал - капитал, необходимый для покрытия существенных рисков, в том числе потенциальных, принятых банком, рассчитанный внутри банка с использованием собственных моделей;

При применении требований Правил к филиалу банка-нерезидента Республики Казахстан:

под советом директоров понимается соответствующий орган управления банка-нерезидента Республики Казахстан;

под правлением понимаются руководящие работники филиала банка-нерезидента Республики Казахстан;

под собственным капиталом понимаются активы филиала банка-нерезидента Республики Казахстан, принимаемые в качестве резерва, рассчитанные в соответствии с требованиями Постановления № 23;

под финансовой отчетностью понимается отчетность по данным бухгалтерского учета филиала банка-нерезидента Республики Казахстан;

под главой риск-менеджмента понимается руководитель подразделения по управлению рисками филиала банка-нерезидента Республики Казахстан;

под главным комплаенс-контроллером понимается руководитель подразделения по комплаенс-контролю филиала банка-нерезидента Республики Казахстан.»;

пункт 97 изложить в следующей редакции:

«97. Политика и процедуры управления риском ОД/ФТ включают, но, не ограничиваясь, следующее:

1) разработку и исполнение внутренних документов, регламентирующих порядок управления риском ОД/ФТ, осуществления финансового мониторинга и внутреннего контроля в целях противодействия ОД/ФТ;

2) методику оценки рисков ОД/ФТ в соответствии с правилами банка по внутреннему контролю для целей противодействия ОД/ФТ;

3) внутренний порядок организации управления рисками банка в разрезе его структурных подразделений и (или) работников в части ОД/ФТ;

4) наличие программы принятия и обслуживания клиентов (customer acceptance policy);

5) банк при разработке и реализации процедур принятия решения о приеме клиента на обслуживание учитывает факторы риска, в том числе выявленные и размещенные на интернет-ресурсе уполномоченного органа.

Внутренние процедуры и порядок отказа от установления и прекращения деловых отношений с клиентом разрабатываются с учетом факторов риска, размещенных на интернет-ресурсе уполномоченного органа. Информация о фактах отказа в установлении и прекращения деловых отношений направляется в уполномоченный орган ежеквартально, не позднее 5 (пятого) числа месяца следующего за отчетным кварталом;

6) наличие автоматизированной информационной системы, цифровых решений на основе искусственного интеллекта и (или) машинного обучения, применяемых к большим данным, и процедур, которые позволяют выявлять операции, подлежащие финансовому мониторингу, а также позволяют своевременно направлять соответствующие сведения и информацию в уполномоченный орган по финансовому мониторингу.

Требования о наличии цифровых решений на основе искусственного интеллекта и (или) машинного обучения, применяемых к большим данным, в том числе, на основе аутсорсинга, распространяются в отношении банков, отнесенных к системно значимым банкам и потенциально системно значимым банкам в соответствии с постановлением Правления Национального Банка Республики Казахстан от 23 декабря 2019 года № 240 «Об утверждении Правил отнесения финансовых организаций к числу системно значимых», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 19925.

Автоматизированная информационная система, цифровые решения на основе искусственного интеллекта и (или) машинного обучения, применяемые к большим данным, и процедуры банка, указанные в подпункте 6) части первой настоящего пункта, дополнительно обеспечивают выявление и блокирование операций, в том числе с учетом характеристик, соответствующих типологиям, схемам и способам легализации (отмывания) преступных доходов и финансирования терроризма, утвержденным государственным органом, осуществляющим финансовый мониторинг, связанных с:

1) незаконным производством, оборотом и (или) транзитом наркотиков;

2) организацией деятельности финансовых пирамид;

3) осуществлением платежей и переводов денег в пользу бирж цифровых активов, не являющихся участниками Международного финансового центра «Астана», перечень которых формируется уполномоченным органом;

4) осуществлением платежей и (или) переводов денег в пользу электронного казино и интернет-казино.

Цифровые решения на основе искусственного интеллекта и (или) машинного обучения, применяемые к большим данным, обеспечивают, не ограничиваясь:

1) мониторинг и надлежащую проверку клиента, в том числе, поведенческий анализ клиента на основе аналитики больших данных с учетом оценки поведения равноправной категории лиц со схожими характеристиками и в сравнении с предыдущим поведением клиента и характерными для него операциями;

2) использование алгоритмов машинного обучения для обнаружения аномалий и определения критериев подозрительных операций с признаками мошенничества или иных противоправных инцидентов, мошенничества или иных противоправных инцидентов на основе анализа исторических данных по имевшим место мошенническим операциям и операциям, связанным с иными противоправными инцидентами;

3) наличие взаимосвязанных систем мониторинга транзакций и систем принятия решений в режиме реального времени и их адаптивное обучение с учетом новых схем и критериев подозрительных операций с признаками мошенничества или иных противоправных инцидентов, мошенничества или иных противоправных инцидентов;

4) анализ социальных сетей, внутренних/внешних отчетов и документов, интернет-исследований (веб-скрейпинг), в том числе, путем использования инструментов обработки естественного языка.»;

дополнить пунктом 97-1 следующего содержания:

«97-1. Главный комплаенс-контролер несет ответственность за:

1) соблюдение банком, работниками банка требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, Международных стандартов по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (ФАТФ 40), политик и процедур управления комплаенс-риском, риском ОД/ФТ;

2) внедрение, актуализацию и реализацию действенных политик и процедур управления комплаенс-риском с учетом соразмерности рискам, присущим деятельности банка, и их совершенствование с учетом мировых тенденций;

3) соответствие политик и процедур управления комплаенс-риском, риском ОД/ФТ требованиям законодательства Республики Казахстан и их эффективность в процессах выявления, предотвращения, обнаружения и устранения нарушений;

4) разработку и актуализацию годового плана работ по совершенствованию системы управления комплаенс-риском;

5) подготовку Совету директоров банка ежеквартальных отчетов о состоянии системы комплаенс-контроля, а также предоставление предложений по улучшению системы управления комлпаенс риска;

6) наличие и эффективность программ, направленных на недопущение систематического вовлечения банка, работников банка и услуг банка в противоправные действия, в том числе, связанные с незаконным производством, оборотом и (или) транзитом наркотиков, организацией деятельности финансовых пирамид, осуществлением платежей и (или) переводов денег в пользу электронного казино и интернет-казино;

7) формирование программ поощрения работников по недопущению противоправных действий;

8) проведение анализа и принятие мер в случае возможных нарушений комплаенс требований (политик и процедур управления комплаенс-риском, требований законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма);

9) разработку и внедрение механизмов внутреннего контроля для предотвращения выявления и минимизации нарушений.»;

пункт 98 изложить в следующей редакции:

«98. Банк обеспечивает наличие системы внутреннего контроля, которая соответствует текущей рыночной ситуации, стратегии, объему активов, уровню сложности операций банка. Внутренний контроль - процесс, встроенный в повседневную деятельность, осуществляемую уполномоченными коллегиальными органами банка, структурными подразделениями и всеми работниками банка при исполнении своих обязанностей, и направленный на выполнение следующих целей:

1) обеспечение эффективности деятельности банка, включая эффективность управления банковскими рисками, активами и пассивами, обеспечение сохранности активов;

2) обеспечение полноты, достоверности и своевременности финансовой, регуляторной и другой отчетности для внутренних и внешних пользователей, а также информационной безопасности;

3) обеспечение соблюдения банком требований гражданского, налогового, банковского законодательства Республики Казахстан, законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, законодательства Республики Казахстан о валютном регулировании и валютном контроле, о платежах и платежных системах, о пенсионном обеспечении, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о кредитных бюро и формировании кредитных историй, о коллекторской деятельности, об обязательном гарантировании депозитов, о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, об акционерных обществах, внутренних документов банка;

4) недопущение вовлечения банка и его работников, клиентов банка:

в осуществление противоправной деятельности, в том числе мошенничества, обмана, ОД/ФТ, незаконного производства, оборота и (или) транзита наркотиков, организацию деятельности финансовых пирамид, осуществление платежей и (или) переводов денег в пользу электронного казино и интернет-казино; осуществление операций, связанных с проведением операций, имеющих высокий риск ОД/ФТ;

в осуществление операций, связанных с дальнейшим приобретением необеспеченных цифровых активов на биржах цифровых активов, не являющихся участниками Международного финансового центра «Астана», перечень которых формируется уполномоченным органом;

в осуществление платежей и (или) переводов денег в пользу электронного казино и интернет-казино;

в осуществление платежей и (или) переводов денег физическими лицами, не достигшими возраста двадцати одного года, в пользу организатора игорного бизнеса.

Банк осуществляет оценку риска ОД/ФТ в случае наличия подозрений о том, что деловые отношения используются клиентом в рамках иных противоправных инцидентов, а также в отношении клиентов, являющихся:

1) держателями пяти и более платежных карточек, выпущенных одним банком, за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса Республики Казахстан, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов;

2) держателями пяти и более платежных карточек, выпущенных в совокупности несколькими банками (при наличии у банка таких сведений посредством обмена данными с иными банками и (или) антифрод-центром НБРК), за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса Республики Казахстан, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов;

3) резидентами стран с высоким риском ОД/ФТ на основе фактора незаконного производства, оборота и (или) транзита наркотиков;

4) нерезиденты Республики Казахстан, не имеющие вид на жительство иностранца в Республике Казахстан либо разрешение на постоянное проживание (не проживающие на территории Республики Казахстан);

5) относящимися к категории лиц в возрасте от четырнадцати лет двадцати пяти лет, при наличии одного из следующих условий:

отсутствие официальных источников доходов (заработная плата, стипендии, алименты, пособия и социальные выплаты, выплаты целевых накоплений из единого накопительного пенсионного фонда в целях улучшения жилищных условий и (или) оплаты образования и иные официальные источники доходов), наличие поступлений крупных сумм от лиц, не связанных родственными отношениями с клиентом, и проведение по банковскому счету частых внутристрановых переводов в адрес третьих физических лиц, трансграничных платежей и (или) переводов денег;

отсутствие по банковскому счету операций, связанных с обеспечением жизнедеятельности клиента, коммунальных платежей, налоговых и иных платежей в бюджет, и проведение по банковскому счету частых внутристрановых переводов в адрес третьих физических лиц, трансграничных платежей и (или) переводов денег;

6) вовлеченными в осуществление платежей и переводов денег в пользу бирж цифровых активов, не являющихся участниками Международного финансового центра «Астана», перечень которых формируется уполномоченным органом;

7) держателями платежных карточек, выданных через расчетно-кассовые отделения или электронно-механические устройства банков, предназначенные для получения электронных банковских услуг, расположенные в приграничных территориях Республики Казахстан.

В отношении клиентов, указанных в части второй настоящего пункта, банк присваивает высокий уровень риска ОД/ФТ, применяет усиленные меры надлежащей проверки таких клиентов и отвечает за:

обеспечение проведения проверки источника происхождения средств клиентов банка;

принятие мер, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, при выявлении подозрительных операций;

осуществление мониторинга и изучение всех операций клиента;

принятие мер в отношении нерезидентов Республики Казахстан по установлению цели и характера деловых отношений путем затребования документов, подтверждающих обоснованность нахождения в Республике Казахстан в соответствии с постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 22 марта 2020 года № 18 «Об утверждении Требований к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан и Национального оператора почты», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 20106. Требования настоящего абзаца применяются в отношении нерезидентов Республики Казахстан, определенных в подпункте 3) части второй настоящего пункта, и иных нерезидентов Республики Казахстан – клиентов банка, в отношении которых имеются подозрения о подверженности высокому риску ОД/ФТ, рискам мошенничества и иных противоправных инцидентов;

обновление сведений о клиенте (его представителе) в соответствии с требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

направление информации в уполномоченный орган по финансовому мониторингу по клиентам банка;

прекращение деловых отношений с клиентами банка в случаях, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Банк осуществляет выявление и блокирование платежей и переводов денег в пользу бирж цифровых активов, не являющихся участниками Международного финансового центра «Астана», перечень которых формируется уполномоченным органом.

В отношении участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, банк осуществляет оценку риска ОД/ФТ. При присвоении участнику Международного финансового центра «Астана», оказывающему услуги по управлению платформой цифровых активов, высокого уровня риска ОД/ФТ банк применяет усиленные меры надлежащей проверки клиентов, а также при проведении банковских операций отвечает за:

проведение оценки степени подверженности услуг (продуктов), предоставляемых участнику Международного финансового центра «Астана», оказывающему услуги по управлению платформой цифровых активов, рискам ОД/ФТ;

проведение процедур по надлежащей проверке при установлении деловых отношений, которые включают помимо мер по надлежащей проверке, предусмотренных для клиентов, дополнительно меры по получению и фиксированию сведений о репутации и характере деятельности участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, применении в отношении него мер со стороны Комитета Международного финансового центра «Астана» по регулированию финансовых услуг;

прекращение деловых отношений с участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, в случаях, выявления банком фактов использования участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, счетов, находящихся в банке-ширме;

отказ в установлении или прекращение деловых отношений с участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, учредители которого зарегистрированы на территории иностранного государства:

включенного в перечень государств (территорий), не выполняющих либо недостаточно выполняющих рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФAТФ), составляемый уполномоченным органом по финансовому мониторингу;

в отношении которого применяются международные санкции в соответствии с резолюциями Совета Безопасности Организации Объединенных Наций;

включенного в перечень офшорных зон в соответствии с постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 24 февраля 2020 года № 8 «Об установлении Перечня офшорных зон для целей банковской и страховой деятельности, деятельности профессиональных участников рынка ценных бумаг и иных лицензируемых видов деятельности на рынке ценных бумаг, деятельности акционерных инвестиционных фондов и деятельности организаций, осуществляющих микрофинансовую деятельность», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 20095;

определенного банком в качестве представляющего высокий риск ОД/ФТ на основе других факторов (сведений об уровне коррупции, незаконного производства, оборота и (или) транзита наркотиков, сведений о поддержке международного терроризма и другое).

осуществление мониторинга и изучение операций с деньгами участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, а также предотвращение незаконного вывода средств за рубеж, в том числе в офшорные зоны;

принятие мер, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, при выявлении подозрительных операций с деньгами и (или) иным имуществом (далее - подозрительные операции);

прекращение деловых отношений с участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, в случаях, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

обеспечение проведения проверки источника происхождения средств участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, при пополнении банковского счета;

обеспечение хранения записи транзакций по операциям с деньгами и предоставление информации в уполномоченный орган по финансовому мониторингу;

обеспечение хранения не менее пяти лет документов, данных и (или) сведений, полученных и собранных в рамках надлежащей проверки участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

осуществление проверки принадлежности и (или) причастности участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, и его бенефициарного собственника к публичному должностному лицу, его супруге (супругу) и близким родственникам в случаях, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, или финансированию терроризма;

представление в уполномоченный орган по финансовому мониторингу необходимой информации при выявлении подозрительных операций в сроки, установленные требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, или финансированию терроризма.

В отношении клиентов банка, осуществляющих операции с участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, банк при проведении разовых банковских операций в сумме, не превышающей 1 000 (одну тысячу) долларов США в эквиваленте по рыночному курсу обмена валют на дату проведения банковской операции, применяет упрощенные меры надлежащей проверки клиентов, за исключением случаев совершения клиентами подозрительных операций.

В отношении клиентов банка, осуществляющих операции с участником Международного финансового центра «Астана», оказывающим услуги по управлению платформой цифровых активов, банк при проведении разовых банковских операций в сумме, равной или превышающей 1 000 (одну тысячу) долларов США в эквиваленте по рыночному курсу обмена валют на дату проведения банковской операции, применяет усиленные меры надлежащей проверки клиентов и отвечает за:

обеспечение проведения проверки источника происхождения средств клиентов банка при осуществлении перевода в пользу участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

принятие мер, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, при выявлении подозрительных операций;

осуществление мониторинга и изучение операций с деньгами клиентов банка, а также предотвращение незаконного вывода средств за рубеж, в том числе в офшорные зоны;

прекращение деловых отношений с клиентами банка в случаях, установленных требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

При открытии банковского счета для обслуживания операций клиентов участник Международного финансового центра «Астана», оказывающий услуги по управлению платформой цифровых активов, представляет следующие документы:

лицензия участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, на оказание финансовой услуги по управлению платформой цифровых активов, выданная Комитетом Международного финансового центра «Астана» по регулированию финансовых услуг;

выписка из реестра, подтверждающая регистрацию в качестве участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

бизнес-план и бизнес-модель участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

политика по противодействию ОД/ФТ участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

приказ о назначении руководителя участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов;

информация об исполнительном органе участника Международного финансового центра «Астана», оказывающего услуги по управлению платформой цифровых активов, и его руководителе (документ, удостоверяющий его личность, подтверждение данных о месте жительства, рекомендательные письма, сведения об отсутствии неснятой или непогашенной судимости).

Эффективный внутренний контроль обеспечивается путем формирования надлежащего управленческого контроля и культуры контроля (контрольной среды).

Управленческий контроль и культура контроля (контрольная среда) характеризуют общее отношение, осведомленность и практические действия совета директоров банка и правления банка, направленные на создание и эффективное функционирование системы внутреннего контроля.»;

пункт 103 изложить в следующей редакции:

«103. Система внутреннего контроля обеспечивает контроль над своевременным выявлением и оценкой на постоянной основе рисков, присущих банку, и принятием своевременных мер по минимизации существенных рисков в соответствии с внутренними документами банка и с учетом международных, страновых, наднациональных санкций. Система внутреннего контроля обеспечивает, но не ограничивается следующим:

1) рассмотрение и учет в ходе оценки рисков внутренних факторов (сложность организационной структуры банка, характер его деятельности, качественные характеристики персонала, организационные изменения, текучесть кадров), а также внешних факторов (изменения экономических условий и ситуации в банковской сфере, технологические новшества), которые негативно сказываются на достижении поставленных банком целей;

2) осуществление оценки рисков по отдельным направлениям деятельности банка;

3) проведение банком новых операций и услуг при условии наличия их регламентации во внутренних документах банка;

4) обеспечение своевременного информирования лиц (подразделений, органов банка), определенных в соответствующих внутренних документах банка, о факторах, влияющих на уровень подверженности банка рискам.

Система внутреннего контроля подвергается корректировке по мере выявления любых новых или неконтролируемых существенных рисков, в том числе связанных с внедрением новых услуг и продуктов.»;

заголовок главы 15 изложить в следующей редакции:

«Глава 15. Управление рисками мошенничества и иных противоправных инцидентов при предоставлении финансовых услуг физическим лицам»;

пункты 121, 122, 123 и 124 изложить в следующей редакции:

«121. Совет директоров банка обеспечивает наличие эффективной системы управления рисками мошенничества и иных противоправных инцидентов, которая соответствует рыночной ситуации, стратегии, объему активов, уровню сложности операций банка и обеспечивает эффективное выявление, измерение, мониторинг и контроль с целью противодействия мошенничеству и иным противоправным инцидентам при использовании банковских услуг и включает, но не ограничиваясь, следующее:

1) политику и процедуры по борьбе с мошенничеством и иными противоправными инцидентами;

2) систему управленческой отчетности;

3) информационные технологии, в том числе антифрод-систему банка.

122. В функции подразделений банка в рамках управления рисками мошенничества и иных противоправных инцидентов входит, но не ограничиваясь, следующее:

1) разработка плана мероприятий по реализации стратегии банка по противодействию мошенничеству и иным противоправным инцидентам, который раскрывает, но, не ограничивается, следующим:

определение потребностей в ресурсах, в том числе определение бюджета, необходимого для реализации процессов противодействия мошенничеству и иным противоправным инцидентам;

описание требуемых мероприятий по противодействию мошенничеству и иным противоправным инцидентам с указанием сроков и ответственных за их реализацию;

2) разработка и внедрение превентивных способов, моделей, технологий и процессов противодействия мошенничеству и иным противоправным инцидентам в отношении клиентов банка на внешних каналах обслуживания и совершенного работниками банка;

3) внедрение, обеспечение, функционирование и непрерывное улучшение процессов противодействия мошенничеству и иным противоправным инцидентам, цифровых каналов предоставления финансовых продуктов и (или) услуг;

4) оценка бизнес-процессов и внедряемых финансовых продуктов и (или) услуг на предмет рисков мошенничества и иных противоправных инцидентов;

5) обеспечение соответствия регуляторным требованиям в сфере противодействия мошенничеству и иным противоправным инцидентам при предоставлении финансовых продуктов и (или) услуг, разработка и последующая методологическая поддержка при установлении контрольных процедур во внутренних документах банка;

6) выявление и аналитика внешних и внутренних данных, а также предупреждение новых схем мошенничества и иных противоправных инцидентов;

7) разработка типологии подозрительных операций с признаками мошенничества или иных противоправных инцидентов;

8) формирование списков лиц, осуществляющих подозрительные операции с признаками мошенничества или иных противоправных инцидентов, списка дропперов, в том числе, мошенников, лиц, связанных с иными противоправными инцидентами;

9) осуществление мониторинга подозрительных операций с признаками мошенничества или иных противоправных инцидентов, поведения клиентов, работников и третьих лиц с признаками мошенничества или иных противоправных инцидентов;

10) ведение и непрерывное обновление базы данных инцидентов;

11) передача данных о подозрительных операциях с признаками мошенничества или иных противоправных инцидентов в антифрод-центр НБРК в круглосуточном режиме и непрерывное обогащение новой информацией по мере появления;

12) обеспечение взаимодействия с антифрод-центром НБРК в соответствии с постановлением Правления Национального Банка Республики Казахстан от 16 июля 2024 года № 43 «Об утверждении Требований к порядку осуществления деятельности центра обмена данными по платежным транзакциям с признаками мошенничества и его взаимодействия с лицами, участвующими в его деятельности», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 34772 (далее – Постановление № 43);

13) обеспечение повышения осведомленности клиентов банка, работников банка и третьих сторон в области противодействия мошенничеству и иным противоправным инцидентам, путем постоянного (периодического) информирования;

14) выявление, фиксация и анализ фактов внутреннего и внешнего мошенничества;

15) участие во внутренних проверках, выработка корректирующих мер и рекомендаций по результатам внутренних проверок, контроль их реализации и составление заключений по результатам внутренней проверки;

16) подготовка предложений для принятия коллегиальным органом решений по вопросам противодействия мошенничеству и иным противоправным инцидентам, в том числе по возмещению ущерба или списания кредита в случае неисполнения банком собственных алгоритмов и моделей оценки риска мошенничества, при проведении операции, выдаче займа (при необходимости);

17) подготовка и предоставление управленческой отчетности о реализации рисков мошенничества и иных противоправных инцидентов, а также об устранении их последствий в соответствии с внутренними документами.

123. Подразделения банка в рамках управления рисками мошенничества и иных противоправных инцидентов разрабатывают внутренний документ, определяющий порядок управления рисками мошенничества и иных противоправных инцидентов, который включает, но не ограничиваясь, следующие процедуры:

1) идентификации рисков мошенничества и иных противоправных инцидентов и определение индикаторов раннего обнаружения подверженности рискам мошенничества и иных противоправных инцидентов;

2) оценки вероятности и последствий всех выявленных рисков мошенничества и иных противоправных инцидентов, применяя качественные и (или) количественные методы оценки, в том числе на основании данных об их реализации;

3) сбора и хранения сведений о реализации существенных рисков мошенничества и иных противоправных инцидентов;

4) формирования реестра рисков, включающего риски мошенничества и иных противоправных инцидентов;

5) разработки мер минимизации рисков мошенничества и иных противоправных инцидентов;

6) мониторинга исполнения мер по обработке рисков мошенничества и иных противоправных инцидентов.

124. Антифрод-система банка отвечает следующим требованиям:

1) обеспечивает техническую интеграцию с антифрод-центром НБРК;

2) обеспечивает полноту отражения информации о подозрительных операциях с признаками мошенничества или иных противоправных инцидентов, мошенничестве или иных противоправных инцидентах, выявленных дропперах в базе данных инцидентов;

3) использует заданные алгоритмы сценариев, модели и правила для выявления подозрительной активности;

4) обеспечивает: ведение внутренних списков лиц, осуществляющих подозрительные операции с признаками мошенничества или иных противоправных инцидентов;

автоматическую сверку с внутренними списками банка, включая списки антифрод-центра НБРК для всех транзакций;

при наличии распоряжения заемщика о перечислении займа на счет третьего лица автоматическое подтверждение через антифрод-центр НБРК со стороны банка-получателя об отсутствии бенефициара платежа во внутренних списках банка-получателя по лицам, осуществляющим подозрительные операции с признаками мошенничества;

5) предусмотрена возможность приостановить и (или) отклонить транзакцию;

6) обеспечивает хранение и безопасность данных, безопасность информационного обмена данными о мошенничестве или иных противоправных инцидентов, в соответствии с постановлением № 48;

7) обеспечивает анализ и настройку параметров для выявления подозрительных операций с признаками мошенничества или иных противоправных инцидентов, тестирование и внесение изменений в антифрод-систему банка.»;

дополнить пунктом 124-1 следующего содержания:

«124-1. Банк обеспечивает непрерывную передачу в антифрод-центр НБРК в круглосуточном режиме по формам, установленным внутренними документами оператора антифрод-центра НБРК:

1) сведений, предусмотренных подпунктом 2) пункта 124 Правил;

2) сведений по выпущенным платежным карточкам, которые включают, но не ограничиваясь, сведения о держателе и реквизитах платежной карточки (при выпуске дополнительных платежных карточек детям дополнительно представляются сведения о родителях или иных законных представителях детей), наименование системы и вид платежной карточки, IP-адресах, абонентском номере сотовой связи, параметрах абонентского устройства сотовой связи (идентификатор, язык, часовой пояс), адрес расположения расчетно-кассового отделения или электронно-механические устройства банка, где выдана платежная карточка, уровне риска клиента (в целях формирования Единой базы платежных карточек на базе антифрод-центра НБРК);

3) сведений об операциях, совершенных с использованием платежной карточки (входящие и исходящие транзакции), которые включают, но не ограничиваясь, сведения о держателе и реквизитах платежной карточки, наименование системы и вид платежной карточки, вид операции (безналичные платежи и (или) переводы денег, операции с наличными деньгами), сведения о платежных реквизитах, в том числе, КНП и назначение платежа, источнике происхождения денег, среде проведения операции (наименование электронного терминала или системы удаленного доступа), при проведении платежа и (или) перевода денег посредством системы удаленного доступа: IP-адресе, абонентском номере сотовой связи, параметрах абонентского устройства сотовой связи (идентификатор, язык, часовой пояс), с использованием которых осуществлен платеж и (или) перевод денег.»;

пункт 125 изложить в следующей редакции:

«125. Политика и процедуры управления рисками мошенничества и иных противоправных инцидентов включают, но не ограничиваются, следующим:

1) оценку рисков мошенничества и иных противоправных инцидентов, при взаимоотношениях с сотрудниками, клиентами и третьими лицами, которые позволяют предотвратить установление отношений, не отвечающих требованиям;

2) перечень операций, подлежащих рассмотрению;

3) критерии подозрительных операций с признаками мошенничества или иных противоправных инцидентов, мошенничества или иных противоправных инцидентов, устанавливаемые в том числе уполномоченным органом;

4) порядок выявления дропперов и приостановления им предоставления электронных банковских услуг в соответствии с пунктом 125-1 Правил;

5) критерии включения и исключения в списки лиц, осуществляющих подозрительные операции с признаками мошенничества или иных противоправных инцидентов, списки мошенников или лиц, связанных с противоправными инцидентами;

6) способы, методы и модели оценки рисков мошенничества и иных противоправных инцидентов, отвечают следующим требованиям:

качественные и количественные методы оценки;

способы, методы и модели должны быть адаптированы к новым методам мошенничества и иных противоправных инцидентов, уровню сложности операций банка, а также изменениям в процессах банка и в законодательстве;

системы обнаружения мошенничества и иных противоправных инцидентов, для выявления аномалий в транзакционных и нетранзакционных данных, а также поведения клиентов и сотрудников, которые могут свидетельствовать о подозрительных операциях и мошенничестве, иных противоправных инцидентах, обеспечивают проверку в автоматическом режиме;

7) порядок взаимодействия подразделений банка и передача данных в соответствии с правилами антифрод-центра НБРК;

8) порядок проведения периодического обучения и аттестации работников по вопросам противодействия мошенничеству и иным противоправным инцидентам;

9) порядок аутентификации, который включает, но не ограничиваясь:

проверку подлинности учетных данных клиентов, работников и третьих лиц;

инструкции по обеспечению защиты информационного актива и предотвращению несанкционированного доступа или действий;

10) порядок предотвращения, учитывающий как внутренние, так и внешние риски мошенничества и иных противоправных инцидентов, влияющие на банк;

11) порядок обнаружения, который включает, но не ограничиваясь:

источники данных, используемые для выявления подозрительных действий клиента и подозрительных операций с признаками мошенничества или иных противоправных инцидентов;

системы и технологии контроля, внедренные для выявления подозрительных операций с признаками мошенничества или иных противоправных инцидентов, оповещения о важных событиях или транзакциях, в том числе руководящих работников, подразделений банка;

роли и обязанности подразделений и работников при обнаружении подозрительных операций с признаками мошенничества или иных противоправных инцидентов;

12) план реагирования на фактический или предполагаемый инцидент с мошенничеством или иной противоправный инцидент, который включает, но не ограничиваясь:

режим работы сотрудников, обеспечивающий непрерывность реагирования;

перечень случаев приостановления и возобновления или отклонения транзакции;

принятие решения о необходимости проведения внутреннего расследования;

13) порядок расследования, который включает, но не ограничивается:

порядок взаимодействия подразделений банка;

оценка срочности, существенности, сбор и анализ информации;

документирование предпринятых следственных действий;

оценка факта мошенничества или иного противоправного инцидента и дата завершения расследования;

принятые меры, в том числе по возмещению ущерба клиенту, если применимо;

14) оценку эффективности системы управления рисками мошенничества и иных противоправных инцидентов, в том числе службой внутреннего аудита банка.»;

дополнить пунктом 125-1 следующего содержания:

«125-1. Банк определяет порядок выявления дропперов и приостановления им предоставления электронных банковских услуг посредством использования автоматизированной информационной системы, цифровых решений на основе искусственного интеллекта и (или) машинного обучения, применяемых к большим данным, и процедур, указанных в подпункте 6) части первой пункта 97 Правил, в том числе, с использованием сведений, полученных при взаимодействии с Антифрод-центром НБРК.

Порядок выявления дропперов включает процедуры выявления операций клиента, имеющих характеристики, соответствующие типологии, утвержденной уполномоченным органом по финансовому мониторингу, в том числе, но не ограничиваясь, соответствующих следующим признакам:

1) клиенты банка, включенные или участвовавшие в операциях с лицами, включенными в списки лиц антифрод-центра НБРК, осуществляющих подозрительные операции с признаками мошенничества или иных противоправных инцидентов, и списки мошенников или лиц, связанных с иными противоправными инцидентами;

2) клиенты банка, участвовавшие в операциях с лицами, включенными во внутренние списки лиц, осуществляющих подозрительные операции с признаками мошенничества или иных противоправных инцидентов;

3) клиенты банка, использующие один абонентский номер сотовой связи совместно с другими клиентами банка и (или) клиентами других банков либо абонентский номер сотовой связи, зарегистрированный в базе мобильных граждан за другим физическим лицом;

4) клиенты банка, использующие одно абонентское устройство связи либо IP-адрес для доступа к электронным банковским услугам совместно с другими клиентам банка;

5) несоответствие характера, и (или) параметров, объема операции клиента (время, дни осуществления операции, геолокация клиента, абонентское устройство сотовой связи или IP-адрес, с использованием которого осуществляется операция, сумма операции, периодичность (частота) осуществления операции, бенефициар, назначение платежа, источник происхождения денег), операциям, обычно совершаемым клиентом в повседневной практике.

При выявлении дроппера при риске мошенничества банк незамедлительно приостанавливает предоставление клиенту электронных банковских услуг, в соответствии с Законом Республики Казахстан «О платежах и платежных системах», Постановлением № 43 отказывает в исполнении платежа и (или) перевода денег либо приостанавливает и (или) блокирует сумму денег по платежу и (или) переводу денег на срок не более трех рабочих дней, информирует клиента в порядке и способами, предусмотренном банком, направляет уведомление в антифрод-центр НБРК. Возобновление операций клиента осуществляется в порядке. установленном Постановлением № 43, с одновременным предоставлением (возобновлением) доступа к электронным банковским услугам.

При выявлении дроппера при рисках иных противоправных инцидентов банк:

1) незамедлительно приостанавливает предоставление клиенту электронных банковских услуг;

2) направляет информацию в антифрод-центр НБРК и уполномоченный орган по финансовому мониторингу с указанием сведений о клиенте, платежных реквизитов по входящим и исходящим платежам и (или) переводам денег, источнике происхождения денег, геолокации клиента, IP-адресе, абонентском номере сотовой связи, параметре абонентского устройства сотовой связи (идентификатор, язык, часовой пояс), с использованием которых проведены операции по банковскому счету, в случае предоставления электронных банковских услуг;

3) возобновляет предоставление электронных банковских услуг в соответствии с порядком приостановления предоставления электронных банковских услуг дропперам, в том числе, при исключении лица из баз антифрод-центра НБРК в соответствии с Постановлением № 43.»;

пункт 126 изложить в следующей редакции:

«126. Управленческая информация содержит, но не ограничивается, следующим:

1) результаты оценки рисков мошенничества и иных противоправных инцидентов, показатели склонности к рискам мошенничества и иных противоправных инцидентов, соответствие пороговым значениям и лимитам;

2) количественный и качественных анализ подозрительных операций с признаками мошенничества или иных противоправных инцидентов в разрезе продуктов банка и типа платежа (если применимо) с указанием типологии мошенничества и иных противоправных инцидентов;

3) принятые меры по фактам мошенничества и иных противоправных инцидентов;

4) операционные убытки банка, связанные с внутренним и внешним мошенничеством или иными противоправными инцидентами и размер возмещения убытков потребителям;

5) объем обращений о мошенничестве и иных противоправных инцидентов в разрезе продуктов банка и типа платежа (если применимо).».

3. Внести в [постановление](http://online.zakon.kz/Document/?doc_id=39795745) Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 22 марта 2020 года № 18 «Об утверждении Требований к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан и Национального оператора почты» (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 20160) следующие изменения и дополнения:

в Требованиях к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан и Национального оператора почты, утвержденных указанным постановлением:

пункт 2 изложить в следующей редакции:

«2. Если Требованиями не предусмотрено иное, понятия, применяемые в Требованиях, используются в значениях, указанных в Законе о ПОД/ФТ, Законе Республики Казахстан «О платежах и платежных системах» и Законе Республики Казахстан «Об акционерных обществах».

Для целей Требований используются следующие понятия:

1) необычная операция (сделка) - операция (сделка) клиента, подлежащая обязательному изучению в соответствии с пунктом 4 статьи 4 Закона о ПОД/ФТ с учетом признаков определения подозрительной операции, определенных уполномоченным органом, осуществляющим финансовый мониторинг и принимающим иные меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, финансированию распространения оружия массового уничтожения (далее - уполномоченный орган по финансовому мониторингу) в соответствии с пунктом 2 статьи 10 Закона о ПОД/ФТ, а также разработанных банком самостоятельно;

2) разовая операция (сделка) - предоставление банком услуг путем проведения операций по зачислению денег на банковский счет физического лица либо проведению платежа в пользу поставщика услуг посредством оборудования (устройства), предназначенного для приема наличных денег, безналичному платежу или переводу денег без использования банковского счета, покупке, продаже или обмену наличной иностранной валюты в обменном пункте, использованию платежной карточки, не являющейся средством доступа к банковскому счету такого клиента, оплате задолженности в рамках исполнительного производства в пользу государственных органов посредством оборудования (устройства), покупке аффинированного золота в слитках через обменные пункты, а также предоставление банком услуг не идентифицированным владельцам электронных денег путем проведения операций по приобретению и использованию электронных денег;

3) дроппер - лицо, предоставившее третьему лицу доступ к своему банковскому счету и (или) средству электронного платежа, а равно передавшее свои платежные инструменты в пользование третьему лицу, в том числе, за материальное вознаграждение, повлекшее их несанкционированное использование в противоправных операциях;

4) управление рисками ОД/ФТ - совокупность принимаемых банком мер по выявлению, оценке, мониторингу рисков ОД/ФТ, а также их минимизации (в отношении услуг (продуктов), клиентов, а также совершаемых клиентами операций);

5) клиент - физическое, юридическое лицо или иностранная структура без образования юридического лица, получающие услуги банка;

6) риски легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения (далее - риски ОД/ФТ) - риски преднамеренного или непреднамеренного вовлечения банка в процессы легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения (далее - ОД/ФТ) или иную преступную деятельность;

7) цифровой актив - имущество, созданное в электронно-цифровой форме с применением средств криптографии и компьютерных вычислений, не являющееся финансовым инструментом, а также электронно-цифровая форма удостоверения имущественных прав;

8) пороговая операция - операция клиента с деньгами и (или) иным имуществом, которая в соответствии с пунктом 1 статьи 4 Закона о ПОД/ФТ подлежит финансовому мониторингу;

9) деловые отношения - отношения по предоставлению банком клиенту услуг (продуктов), относящихся к финансовой деятельности и финансовым услугам.»;

пункт 15 изложить в следующей редакции:

«15. Типы клиентов, чей статус и (или) чья деятельность повышают риск ОД/ФТ, включают, но не ограничиваются:

1) публичные должностные лица, их супруги и близкие родственники;

2) иностранные финансовые организации;

3) юридические лица и индивидуальные предприниматели, деятельность которых связана с интенсивным оборотом наличных денег, в том числе:

юридические лица, осуществляющие деятельность исключительно через обменные пункты на основании лицензии Национального Банка Республики Казахстан на обменные операции с наличной иностранной валютой;

юридические лица, исключительной деятельностью которых является инкассация банкнот, монет и ценностей на основании лицензии Национального Банка Республики Казахстан (за исключением дочерних организаций банков, которые соблюдают требования по ПОД/ФТ, установленные банком);

организации, осуществляющие микрофинансовую деятельность;

агенты (поверенные) поставщиков услуг (кроме финансовых), осуществляющие прием от потребителей наличных денег, в том числе через электронные терминалы;

организаторы игорного бизнеса, а также лица, предоставляющие услуги либо получающие доходы от деятельности онлайн-казино за пределами Республики Казахстан;

лица, предоставляющие туристские услуги, а также услуги, связанные с интенсивным оборотом наличных денег;

4) адвокаты и другие независимые специалисты по юридическим вопросам в случаях, когда они от имени или по поручению клиента участвуют в операциях с деньгами и (или) имуществом в отношении деятельности, указанной в подпункте 7) пункта 1 статьи 3 Закона о ПОД/ФТ, профессиональные участники рынка ценных бумаг (за исключением дочерних организаций банков второго уровня, которые соблюдают требования по ПОД/ФТ, установленные банками второго уровня);

5) страховые (перестраховочные) организации, страховые брокеры, осуществляющие деятельность по отрасли «страхование жизни» (за исключением дочерних организаций банка, которые соблюдают требования по ПОД/ФТ, установленные банком);

6) лица, предоставляющие услуги по финансовому лизингу (за исключением дочерних организаций банков второго уровня, которые соблюдают требования по ПОД/ФТ, установленные банками второго уровня);

7) лица, осуществляющие деятельность в качестве страховых агентов;

8) лица, осуществляющие посредническую деятельность по купле-продаже недвижимости;

9) лица, деятельность которых связана с производством и (или) торговлей оружием, взрывчатыми веществами;

10) лица, деятельность которых связана с добычей и (или) обработкой, а также куплей-продажей, драгоценных металлов, драгоценных камней либо изделий из них;

11) некоммерческие организации в организационно-правовой форме фондов, религиозных объединений;

12) лица, расположенные (зарегистрированные) в иностранных государствах, указанных в пункте 17 Требований, а также расположенные в Республике Казахстан филиалы и представительства таких лиц;

13) клиент, в отношении которого имеются основания для сомнения в достоверности полученных данных;

14) клиент совершает действия, направленные на уклонение от процедур надлежащей проверки клиента, предусмотренных Законом о ПОД/ФТ;

15) лица, осуществляющие выпуск и обращение обеспеченных цифровых активов;

16) лица, осуществляющие выпуск и оборот необеспеченных цифровых активов на территории Международного финансового центра «Астана»;

17) клиенты, являющиеся держателями пяти и более платежных карточек, выпущенных одним банком, за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса Республики Казахстан (далее – Гражданский кодекс), дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов;

18) клиенты, являющиеся держателями пяти и более платежных карточек, выпущенных в совокупности несколькими банками (при наличии у банка таких сведений посредством обмена данными с иными банками и (или) антифрод-центром НБРК), за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов;

19) резидентами стран с высоким риском ОД/ФТ на основе фактора незаконного производства, оборота и (или) транзита наркотиков;

20) нерезиденты Республики Казахстан, не имеющие вид на жительство иностранца в Республике Казахстан либо разрешение на постоянное проживание (не проживающие на территории Республики Казахстан);

21) относящимися к категории лиц в возрасте от четырнадцати лет двадцати пяти лет, при наличии одного из следующих условий:

отсутствие официальных источников доходов (заработная плата, стипендии, алименты, пособия и социальные выплаты, выплаты целевых накоплений из единого накопительного пенсионного фонда в целях улучшения жилищных условий и (или) оплаты образования и иные официальные источники доходов), наличие поступлений крупных сумм от лиц, не связанных родственными отношениями с клиентом, и проведение по банковскому счету частых внутристрановых переводов в адрес третьих физических лиц, трансграничных платежей и (или) переводов денег;

отсутствие по банковскому счету операций, связанных с обеспечением жизнедеятельности клиента, коммунальных платежей, налоговых и иных платежей в бюджет, и проведение по банковскому счету частых внутристрановых переводов в адрес третьих физических лиц, трансграничных платежей и (или) переводов денег;

22) клиенты, совершившие в течение последних 6 (шести) месяцев три и более платежей в пользу организатора игорного бизнеса на общую сумму более 300 000 (триста тысяч) тенге;

23) клиенты, являющиеся держателями платежных карточек, выданных через расчетно-кассовые отделения или электронно-механические устройства банков, предназначенные для получения электронных банковских услуг, расположенные в приграничных территориях Республики Казахстан.»;

пункт 18 изложить в следующей редакции:

«18. Услуги (продукты) банка, а также способы их предоставления, повышающие риск ОД/ФТ, включают, но не ограничиваются:

1) новые продукты и новая деловая практика, включая новые механизмы передачи, новые или развивающиеся технологии, как для новых, так и для уже существующих продуктов, определяемые в правилах внутреннего контроля банка;

2) персональное банковское обслуживание клиентов;

3) платежи и (или) переводы денег без использования банковского счета;

4) торговое финансирование;

5) сейфовые операции (услуги по хранению ценных бумаг, выпущенных в документарной форме, документов и ценностей клиентов, включая сдачу в аренду сейфовых ящиков, шкафов и помещений);

6) доверительное управление имуществом;

7) брокерское обслуживание на международных рынках;

8) кастодиальное обслуживание;

9) электронные деньги в случае, если банк-эмитент не является оператором соответствующей системы электронных денег;

10) предоплаченные платежные карточки;

11) корпоративные платежные карточки;

12) чеки, в том числе дорожные чеки;

13) счета иностранных финансовых организаций;

14) операции по покупке, продаже, обмену наличной иностранной валюты через обменные пункты;

15) трансграничные платежи и (или) переводы денег физических лиц на сумму более 500 000 (пятьсот тысяч) тенге.»;

пункт 22 изложить в следующей редакции:

«22. Программа идентификации клиента, его представителя и бенефициарного собственника включает, но не ограничивается:

1) порядок принятия клиентов на обслуживание, включая процедуру, основания и сроки принятия банком решения об отказе в установлении деловых отношений и (или) в проведении операции, а также прекращении деловых отношений;

2) порядок идентификации клиента (его представителя) и бенефициарного собственника, в том числе особенности процедур применения упрощенных и усиленных мер надлежащей проверки клиента;

3) особенности проведения идентификации при установлении корреспондентских отношений с иностранными финансовыми организациями;

4) описание мер, направленных на выявление банком среди клиентов (их представителей) и бенефициарных собственников, находящихся на обслуживании или принимаемых на обслуживание, публичных должностных лиц, их супругов и близких родственников;

5) порядок применения целевых финансовых санкций, проверки клиента (его представителя) и бенефициарного собственника на наличие в перечнях организаций и лиц, связанных с финансированием терроризма и экстремизма, финансированием распространения оружия массового уничтожения, составляемых в соответствии со статьями 12 (далее - Перечень) и 12-1 (далее - Перечень ФРОМУ) Закона о ПОД/ФТ;

6) порядок прекращения действия целевых финансовых санкций при исключении сведений о клиенте (его представителе) и бенефициарного собственника из Перечня и Перечня ФРОМУ;

7) особенности идентификации при дистанционном установлении деловых отношений (без личного присутствия клиента или его представителя);

8) особенности обмена сведениями, полученными в процессе идентификации клиента (его представителя) и бенефициарного собственника, а также хранения и обеспечения конфиденциальности таких сведений, в рамках выполнения требований по ПОД/ФТ, установленных банковским конгломератом, в который входит банк (при наличии);

9) особенности идентификации клиентов путем получения сведений от других финансовых организаций, в том числе идентификации физических и юридических лиц, в пользу или от имени которых брокером (дилером) совершаются операции по своему банковскому счету;

10) порядок проверки достоверности сведений о клиенте (его представителе) и бенефициарном собственнике;

11) требования к форме, содержанию и порядку ведения досье клиента, обновления сведений, содержащихся в досье, с указанием периодичности обновления сведений;

12) порядок оценки уровня риска клиента, основания оценки такого риска;

13) порядок получения и представления по запросу банка сведений о бенефициарных собственниках клиентов по форме и порядке, определенным уполномоченным органом по финансовому мониторингу в соответствии с частями третьей и четвертой пункта 5 статьи 5 Закона о ПОД/ФТ;

14) порядок проверки клиента (его представителя) и бенефициарного собственника на принадлежность к иностранным организаторам игорного бизнеса, деятельность которых признана незаконной на территории Республики Казахстан на основании судебного акта (далее - иностранные организаторы игорного бизнеса), отказа в проведении платежей и (или) переводов денег в пользу иностранных организаторов игорного бизнеса, а также прекращения деловых отношений с клиентом, являющимся иностранным организатором игорного бизнеса.

Документы, представляемые клиентом (его представителем) в целях подтверждения сведений о клиенте (его представителе) и бенефициарном собственнике, проверяются на их действительность.

В отношении представителя клиента дополнительно проверяются полномочия такого лица действовать от имени и (или) в интересах клиента.

В отношении клиента, с которым банк установил деловые отношения посредством представителя клиента, действующего от имени клиента на основании выданной доверенности, банком до проведения расходных или приходных операций, дополнительно проводится биометрическая идентификация клиента.

При дистанционном установлении деловых отношений с клиентом, при смене клиентом абонентского устройства сотовой связи, используемого для доступа к электронным банковским услугам, банк применяет двухфакторную идентификацию клиента с обязательным проведением биометрической идентификации клиента.

При дистанционном установлении деловых отношений с клиентом и (или) оказании ему электронных банковских услуг банк обеспечивает контроль использования клиентом при проведении операций по банковскому счету, в том числе, с использованием платежной карточки, одного абонентского номера устройства сотовой связи, присвоенного оператором связи – резидентом Республики Казахстан и зарегистрированного за клиентом на веб-портале «электронного правительства» Республики Казахстан для получения государственных и иных услуг (далее – база мобильных граждан).

Предоставление электронных банковских услуг клиенту при использовании мобильного приложения осуществляется через одно абонентское устройство сотовой связи, идентифицированное банком в соответствии с порядком, определенным внутренними правилами банка.

Не допускается дистанционное установление деловых отношений или через представителя с клиентами, относящимся к категории лиц в возрасте от восемнадцати лет до двадцати одного года, а также выпуск и перевыпуск платежной карточки дистанционным способом и (или) через представителя указанным клиентам.

В отношении клиентов, относящихся к категории лиц в возрасте от четырнадцати до восемнадцати лет операции клиента при получении электронных банковских услуг верифицируются родителями или иными законными представителями.

Банк при выпуске клиенту более одной платежной карточки, за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов:

1) запрашивает у клиента цель выпуска дополнительной платежной карточки и сведения о планируемых операциях по банковскому счету;

2) осуществляет мониторинг движения денег по банковскому счету клиента с использованием платежной карточки на предмет соответствия цели выпуска и операциям, указанным клиентом при выпуске платежной карточки.

3) при выявлении прямых несоответствий характера операций клиента по банковскому счету целевому назначению, указанному клиентом при выпуске платежной карточки, банк проводит углубленный мониторинг движения денег по банковскому счету в целях определения необходимости присвоения клиенту высокого уровня риска и проведения усиленных мер надлежащей проверки в соответствии;

4) в случае присвоения клиенту высокого уровня риска проводит мероприятия, предусмотренные Требованиями и постановлением Правления Национального Банка Республики Казахстан от 12 ноября 2019 года № 188 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 19632 (далее – Постановление № 188).

Если банк в соответствии с Законом о ПОД/ФТ на основании договора поручил иному лицу применение в отношении клиентов банка мер, предусмотренных подпунктами 1), 2), 2-1), 2-2) и 4) пункта 3 статьи 5 Закона о ПОД/ФТ, банк разрабатывает правила взаимодействия с такими лицами, которые включают:

процедуру заключения банком договоров с лицами, которым поручено проведение идентификации, а также перечень должностных лиц банка, уполномоченных заключать такие договоры;

процедуру идентификации клиента (его представителя) и бенефициарного собственника в соответствии с договорами между банком и лицами, которым поручено проведение идентификации;

процедуру и сроки передачи банку сведений, полученных при проведении идентификации, лицами, которым поручено проведение идентификации;

процедуру осуществления банком контроля за соблюдением лицами, которым поручено проведение идентификации, требований по идентификации, включая процедуру, сроки и полноту передачи банку полученных сведений, а также меры, принимаемые банком по устранению выявленных нарушений;

основания, процедуру и сроки принятия банком решения об одностороннем отказе от исполнения договора с лицами, которым поручено проведение идентификации, в случае несоблюдения ими требований по идентификации, в том числе процедур, сроков и полноты передачи банку полученных сведений;

перечень должностных лиц банка, уполномоченных принимать решение об одностороннем отказе от исполнения договора с лицами, которым поручено проведение идентификации;

положения об ответственности лиц, которым банк поручил проведение идентификации, за несоблюдение ими требований по идентификации, включая процедуру, сроки и полноту передачи банку полученных сведений;

процедуру взаимодействия банка с лицами, которым поручено проведение идентификации, по вопросам оказания им методологической помощи в целях выполнения требований по идентификации.

Допускается включение банком дополнительных условий в правила взаимодействия.

Банк, поручивший на основании договора иностранной финансовой организации применение мер надлежащей проверки клиентов (их представителей) и бенефициарных собственников, предусмотренных подпунктами 1), 2), 2-1), 2-2) и 4) пункта 3 статьи 5 Закона о ПОД/ФТ, учитывает возможные риски ОД/ФТ.»;

дополнить пунктами 22-1 и 22-2 следующего содержания:

«22-1. В отношении нерезидентов Республики Казахстан, по которым имеются подозрения о подверженности высокому риску ОД/ФТ, рискам мошенничества и иных противоправных инцидентов, за исключением глав, членов персонала дипломатических и приравненным к ним представительств иностранных государств, международных организаций и (или) их представительств, работникам консульских учреждений иностранных государств, а также членам их семей, аккредитованным при Министерстве иностранных дел Республики Казахстан, субъектов предпринимательства, инвесторов:

не допускается дистанционное установление деловых отношений или через представителя, продление таких деловых отношений, а также выпуск и перевыпуск платежной карточки дистанционным способом и (или) через представителя;

при установлении деловых отношений и при смене клиентом абонентского устройства сотовой связи, используемого для доступа к электронным банковским услугам, применение двухфакторной идентификации клиента с обязательным проведением биометрической идентификация клиента с фотоизображением клиента, размещенным в паспорте, с последующим проведением на периодической основе не реже одного раза в месяц подтверждения биометрической идентификации через онлайн-банкинг или мобильное приложение при их применении клиентом;

не допускается выпуск и перевыпуск более одной платежной карточки, за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов;

срок действия выпущенной платежной карточки не превышает 12 (двенадцать) календарных месяцев, за исключением платежных карточек, выпущенных в рамках обслуживания текущих счетов, открытых для целей, предусмотренных подпунктами 1), 2), 2-1), 2-3), 3), 4), 5-1), 5-2), 5-3), 7), 7-1), 8), 9) части второй статьи 741 Гражданского кодекса, дополнительных платежных карточек, выпущенных на имя детей, а также кредитных карточек, по которым осуществляются операции исключительно по выдаче и погашению банковских займов.

Абзацы третий и пятый части первой настоящего пункта применяются в отношении всех нерезидентов Республики Казахстан.

22-2. При открытии банковского счета и выпуске платежной карточки нерезиденту Республики Казахстан банк:

1) проверяет документы клиента, подтверждающие обоснованность нахождения в Республике Казахстан (паспорт с отметкой о пересечении государственной границы Республики Казахстан, регистрационное свидетельство о присвоении индивидуального идентификационного номера, копия заявления, поданного в уполномоченный государственный орган, о выдаче разрешения трудовому мигранту, нотариально заверенная копия трудового договора или договора обучения, нотариально заверенная копия вида на жительство иностранца в Республике Казахстан, копия квитанция об уплате предварительного платежа по индивидуальному подоходному налогу и другие документы);

2) проводит анализ заполненного клиентом опросника, форма которого определяется банком и содержит, не ограничиваясь, сведения о легальности пребывания клиента в Республике Казахстан, подтверждаемые документами клиента в рамках его усиленной надлежащей проверки, цели прибытия в Республику Казахстан, профессиональной деятельности клиента, цели открытия банковского счета (выпуска платежной карточки), источнике финансирования совершаемых операций, при выпуске платежной карточки планируемых трансграничных переводах, планируемом предоставлении доступа к банковскому счету для третьего лица (в том числе, посредством мобильного приложения и онлайн-банкинга), наличии банковских счетов в других банках Республики Казахстан и цели их открытия, IMEI коде абонентского номера сотовой связи клиента, подтверждение клиента о принятии решения об открытии банковского счета самостоятельно без воздействия третьих лиц и наличии регистрации абонентского номера сотовой связи за клиентом в базе мобильных граждан.

Банк в течение трех последовательных месяцев проводит мониторинг движения денег по банковскому счету клиента - нерезидента Республики Казахстан, по которому осуществляются операции с использованием платежной карточки, на предмет соответствия цели открытия банковского счета (выпуска платежной карточки), обозначенной клиентом в опроснике, а также на наличие по банковскому счету платежей и (или) переводов денег, связанных с обеспечением жизнедеятельности клиента, коммунальных платежей и (или) налоговых и других обязательных платежей в бюджет. При выявлении прямых несоответствий характера операций по банковскому счету сведениям, указанным в опроснике, и отсутствии платежей и (или) переводов денег, связанных с обеспечением жизнедеятельности клиента, коммунальных платежей и (или) налоговых и других обязательных платежей в бюджет, на рассмотрение уполномоченного коллегиального органа банка выносится вопрос о необходимости прекращении деловых отношений с клиентом.»;

пункт 27 изложить в следующей редакции:

«27. Периодичность обновления и (или) необходимость получения дополнительных сведений о клиенте (его представителе) и бенефициарном собственнике устанавливаются с учетом уровня риска клиента (группы клиентов) и (или) степени подверженности услуг (продуктов) банка, которыми пользуется клиент, рискам ОД/ФТ.

Обновление сведений о клиенте (его представителе) и бенефициарном собственнике с высоким уровнем риска осуществляется не реже одного раза в год.

Обновление сведений о клиентах (их представителях), указанных в подпунктах 17), 18), 20), 21) и 23) пункта 15 Требований, осуществляется не реже одного раза в квартал.

Обновление сведений о клиенте (его представителе), в отношении которого имеются основания полагать, что его деятельность связана с финансированием незаконным производством, оборотом и (или) транзитом наркотиков, осуществляется не реже одного раза в полгода.»;

пункт 29 изложить в следующей редакции:

«29. Программа мониторинга и изучения операций клиентов включает, но не ограничивается:

1) перечень признаков подозрительных операций, составленный на основе признаков определения подозрительной операции, определенных уполномоченным органом по финансовому мониторингу в соответствии с пунктом 2 статьи 10 Закона о ПОД/ФТ, а также разработанных банком самостоятельно;

2) процедуру выявления операций клиента, имеющих характеристики, соответствующие типологиям, схемам и способам ОД/ФТ, утвержденным уполномоченным органом по финансовому мониторингу в соответствии с пунктом 5 статьи 4 Закона о ПОД/ФТ;

3) распределение обязанностей между подразделениями (работниками) банка по обновлению ранее полученных и (или) получению дополнительных сведений о клиенте (его представителе) и бенефициарном собственнике в случаях, предусмотренных Требованиями;

4) распределение обязанностей между подразделениями (работниками) банка по выявлению и передаче между подразделениями (работниками) сведений о пороговых, необычных и подозрительных операциях;

5) порядок, основания и срок принятия ответственным работником решения о квалификации операции клиента;

6) порядок фиксирования (в том числе способы фиксирования) и хранения сведений о результатах изучения необычных операций (сделок), а также сведений о пороговых и подозрительных операциях (в том числе сумме операции);

7) порядок проведения мониторинга и изучения операций клиентов высокого уровня риска;

8) порядок выявления и анализа непрозрачных трансграничных платежей и (или) переводов денег физических лиц;

9) порядок принятия и описание мер, принимаемых банком в отношении клиента и его операций в случае осуществления клиентом систематически и (или) в значительных объемах необычных и (или) подозрительных операций;

10) порядок представления в уполномоченный орган по финансовому мониторингу сообщений о пороговых и подозрительных операциях;

11) порядок информирования (при необходимости) уполномоченных органов и должностных лиц банка о выявлении пороговой и подозрительной операции.

Для целей признаков определения подозрительных операций, определенных уполномоченным органом по финансовому мониторингу в соответствии с пунктом 2 статьи 10 Закона о ПОД/ФТ, банк в правилах внутреннего контроля самостоятельно определяет оценочные категории (включая, но не ограничиваясь, систематичность, регулярность, значительность, существенность, излишняя озабоченность, необоснованная поспешность, небольшой период, большое количество, группа лиц) с учетом масштаба и основных направлений деятельности банка, характера, масштаба и основных направлений деятельности его клиентов, уровня рисков, связанных с клиентами и их операциями.»;

дополнить пунктами 32-1 и 32-2 следующего содержания:

«32-1. Банк посредством использования автоматизированной информационной системы выявляет клиентов, по банковским счетам которых проводятся расходные операции, при этом отсутствуют платежи, связанные с обеспечением жизнедеятельности клиента, коммунальных платежей, налоговых и иных платежей в бюджет, и направляет в их адрес запрос (опросник) в соответствии с внутренним порядком банка для своевременного представления в сроки, определенные банком, разъяснений о статусе счета, а также проводит повторную двухфакторную идентификацию клиента с обязательным проведением биометрической идентификации клиента.

В случае непредставления клиентом ответа в сроки, определенные банком, банк:

1) принимает решение о необходимости приостановления предоставления клиенту электронных банковских услуг;

2) проводит углубленный мониторинг движения денег по банковскому счету в целях определения необходимости присвоения клиенту высокого уровня риска и проведения в отношении него усиленных мер надлежащей проверки;

3) в случае присвоения клиенту высокого уровня риска проводит мероприятия, предусмотренные Требованиями и Постановлением № 188.

32-2. Порядок выявления и анализа непрозрачных трансграничных платежей и (или) переводов денег физических лиц, включает, но не ограничивается:

1) определение критериев непрозрачных трансграничных платежей и (или) переводов денег, в том числе:

платежи и (или) переводы денег в адрес иностранных структур без образования юридического лица, расположенных в странах с высоким риском ОД/ФТ либо оффшорных зонах, и руководителями либо бенефициарными собственными которых выступают лица, одновременно являющиеся руководителями или бенефициарными собственниками иных иностранных структур без образования юридического лица, расположенных в указанных странах/оффшорных зонах, либо по адресу указанной иностранной структуры без образования юридического лица зарегистрировано несколько иных компаний;

трансграничный безвозмездный перевод в адрес физического лица, который не связан отношениями с отправителем денег;

отсутствие по банковскому счету отправителя денег активных операций до проведения трансграничного платежа и (или) перевода денег более одного года;

характер операций по банковскому счету клиента ограничивается только переводами денег от/в адрес физических лиц и взносами наличных денег;

2) использование автоматизированной информационной системы, цифровых решений на основе искусственного интеллекта и (или) машинного обучения, применяемых к большим данным, для мониторинга трансграничных платежей и (или) переводов денег физических лиц в режиме реального времени;

3) проведение следующих мер, в том числе, посредством оперативного взаимодействия с банками-корреспондентами:

изучение источников финансирования совершаемой операции;

надлежащая проверка отправителя денег и его бенефициарного собственника;

надлежащая проверка получателя денег и его бенефициарного собственника, руководителя получателя денег, за исключением платежей и (или) переводов денег с использованием платежных карточек;

проверка наличия и (или) отсутствия у клиента операций с участием стран с высоким риском ОД/ФТ и стран, включенных в перечень оффшорных зон;

проверка операции на наличие признаков совершения клиентом не имеющей очевидного экономического смысла или видимой законной цели операции с деньгами и (или) иным имуществом;

проверка операции на соответствие характеру платежей и (или) переводов денег, ранее проводимых клиентом по счету.».