УТВЕРЖДЕНО	**УТВЕРЖДЕНО**
Решением единственного участника (Решение № 5 от «26» декабря 2025г.)	Приказом Руководителя/Единоличного исполнительного органа (Приказ № 04 от «26» декабря 2025г.)

ПОЛОЖЕНИЕ (ПРАВИЛА)

управления рисками мошенничества, рассмотрения обращений клиентов

и взаимодействия с Антифрод-центром Национального Банка Республики Казахстан

Наименование документа	Положение (Правила) управления рисками мошенничества, рассмотрения обращений клиентов и взаимодействия с Антифрод-центром НБРК
Версия	1.0
Дата введения в действие	«26» декабря 2025г
Ответственное подразделение	«Комплаенс-служба (ответственный по ПОД/ФТ) под общим контролем Директора»

*Карточка документа

1. Общие положения

1.1. Настоящее Положение (далее - Документ) устанавливает единые требования и процедуры Товарищества с ограниченной ответственностью «Микрофинансовая организация "Кредит Каз Лайн"» (далее-МФО) по выявлению, предотвращению, фиксации и анализу фактов внутреннего и внешнего мошенничества, рассмотрению обращений клиентов и взаимодействию с Антифрод-центром НБРК.

1.2. Документ обязателен для исполнения всеми работниками и подразделениями МФО в части их функций.

1.3. Документ применяется ко всем продуктам и процессам МФО, включая предоставление микрокредитов электронным способом (при применимости), операции по выплате/переводу денег, изменению реквизитов, а также иные операции, подверженные мошенничеству.

1.4. МФО вправе детализировать отдельные процедуры в инструкциях, регламентах и технологических картах при условии соответствия настоящему Документу.

Термины и сокращения

В целях настоящего документа применяются следующие основные термины и сокращения:

Термин/сокращение	Определение
Антифрод-центр НБРК	центр/платформа, обеспечивающая сбор, обработку и обмен сведениями о попытках осуществления платежных транзакций с признаками мошенничества и подтвержденных инцидентах, в порядке, установленном оператором Антифрод-центра.
Антифрод-система	совокупность организационных и технических мер/средств МФО (включая модули в автоматизированной информационной системе), обеспечивающих выявление и предотвращение мошенничества, а также интеграцию и обмен данными с Антифрод-центром (WEB и/или API).
Инцидент	событие, подтвержденное по итогам проверки/расследования, содержащее признаки мошенничества и подлежащее регистрации/учету и (при применимости) передаче в Антифрод-центр.
Подозрительная операция	операция/действие/транзакция, соответствующая индикаторам раннего обнаружения или иным критериям, установленным настоящим документом и (или) внутренними документами МФО.
База данных о попытках	данные Антифрод-центра о попытках осуществления платежных транзакций с признаками мошенничества (в объеме и порядке, доступном МФО как участнику).
WEB	веб-интерфейс Антифрод-центра, предоставляющий доступ уполномоченным пользователям.
стандарт API	Стандарт (требования) взаимодействия API каналов системы «Центр обмена данными по платежным транзакциям с признаками мошенничества (Антифрод-центр)» акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» (для участников)

Роли и ответственность

Для целей управления рисками мошенничества, рассмотрения обращений клиентов и взаимодействия с Антифрод-центром МФО утверждает распределение ролей и ответственности. Конкретные должности/ФИО закрепляются отдельным распорядительным документом (решение единственного участника /приказ) и актуализируются при кадровых изменениях.

Минимально рекомендуемые роли:

- Владелец процесса (ответственный за антифрод): организует систему управления рисками мошенничества; утверждает/актуализирует каталог индикаторов; инициирует пересмотр мер минимизации; формирует отчеты для руководства; контролирует ведение реестров и журналов.
- Функция риск-менеджмента/комплаенс (если выделены отдельно): проводит оценку вероятности и последствий рисков; обеспечивает выполнение внутренних процедур; осуществляет контроль исполнения мер и соблюдения сроков; готовит материалы для проверок.
- Функция информационной безопасности (ИБ): обеспечивает требования по защите информации и персональных данных; устанавливает технические меры (журналирование, контроль доступа, шифрование, мониторинг); участвует в расследованиях и реагировании на инциденты ИБ.
- ИТ / техническая поддержка (внутренняя): настраивает и поддерживает антифрод-правила/интеграции; обеспечивает корректность логирования; поддерживает каналы взаимодействия с Антифрод-центром (WEB/API) и внешними провайдерами.
- Операционное подразделение/кредитный блок: обрабатывает подозрительные операции в части бизнес-процесса (выдача/погашение/вывод); обеспечивает приостановку/ограничение операций при срабатывании индикаторов; документирует решения.
- Контакт-центр/служба поддержки: принимает и регистрирует обращения клиентов о возможном мошенничестве; информирует клиента о статусе рассмотрения; взаимодействует с владельцем процесса и операционным блоком по эскалации.
- Юридическая функция: обеспечивает правовую корректность уведомлений и шаблонов ответов; сопровождает запросы/взаимодействие с госорганами и органами уголовного преследования (при необходимости); контролирует договорные меры (в т.ч. с техническим оператором).
- Уполномоченные пользователи Антифрод-центра: выполняют операции в системе Антифрод-центра в пределах предоставленного доступа; несут персональную ответственность за действия в WEB-интерфейсе и/или в рамках API-процессов.
- Технический оператор (поставщик SaaS-платформы/внешний исполнитель, при наличии): выполняет технические функции по интеграции/обмену данными, настройке антифрод-правил и логированию в пределах договора с МФО; не принимает самостоятельных решений по клиенту; обеспечивает выполнение технических и организационных мер ИБ по требованиям МФО.

Примечание: распределение ответственности по ключевым этапам (RACI) и перечень полномочий/доступов рекомендуется оформить в Приложении (матрица ролей).

Роль	**Функции**
Владелец процесса (Ответственный за антифрод)	обеспечивает актуализацию настоящего документа, координирует расследования, формирует отчетность, инициирует изменения индикаторов и мер.

Служба комплаенс/риск-менеджмента	идентифицирует риски, проводит оценку вероятности/последствий, ведет реестр рисков, контролирует исполнение мер, организует мониторинг KPI.
Служба информационной безопасности (ИБ)	обеспечивает технические и организационные меры защиты, контроль доступов, журналирование, расследование ИБ-инцидентов, участие в антифрод-настройках.
ИТ/Разработчик АИС (в т.ч. внешний поставщик)	реализует правила/интеграции (WEB/API), обеспечивает корректность логирования и сохранность данных, устраняет технические инциденты.
Контакт-центр/служба поддержки	принимает и регистрирует обращения клиентов, выполняет первичные проверки по сценариям, эскалирует обращения для расследования.
Бизнес-подразделения (продукт/операции)	обеспечивают исполнение решений по операциям, информирование клиента, реализацию корректирующих действий по продукту/процессу.
Юридическая служба (при наличии)	сопровождает запросы/взаимодействие с правоохранительными и государственными органами, формирует правовые позиции и шаблоны уведомлений.

Процедура 1. Идентификация рисков мошенничества и индикаторы раннего обнаружения
МФО на постоянной основе идентифицирует риски мошенничества по продуктам, каналам и этапам клиентского пути (онбординг, подача заявки, заключение договора, выдача/перевод денег, погашение, вывод средств, изменение реквизитов и др.).

- Индикаторы раннего обнаружения (Каталог индикаторов, Приложение 1) формируются с учетом:
- данных антифрод-системы и внутренних правил скоринга/фрод-мониторинга;
- результатов сверки с данными Антифрод-центра (в т.ч. базы данных о попытках и иных доступных источников);
- обращений клиентов о мошенничестве и результатов расследований;
- информации от партнеров/платежных организаций (при применимости) и правоохранительных органов.

При срабатывании индикаторов МФО применяет меры реагирования, включая приостановку операции при наличии технической возможности, проведение проверки и принятие решения о регистрации инцидента (разделы 5.4 и 6).

Процедура 2. Оценка вероятности и последствий выявленных рисков мошенничества
Для каждого риска мошенничества МФО определяет вероятность (P) и последствия (I) с использованием качественных и/или количественных методов. Методика оценки приведена в Приложении 2.

- Оценка производится:
- первично - при включении риска в реестр;
- планово - не реже одного раза в квартал;
- внепланово - при существенном инциденте, изменении мошеннических схем или внедрении нового продукта/канала.

При количественной оценке учитываются статистика подтвержденных инцидентов, финансовые потери/возвраты, время обработки кейсов, доля ложноположительных срабатываний, а также данные аудита/проверок.

Процедура 3. Рассмотрение обращений (жалоб) клиентов-физических лиц по вопросам мошенничества

МФО обеспечивает прием, регистрацию и рассмотрение обращений клиентов по вопросам мошенничества по всем доступным каналам. Журнал обращений ведется по форме Приложения 3.

- Минимальные требования:
- регистрация обращения с присвоением уникального номера и фиксацией даты/времени;
- классификация обращения (категория, тип инцидента, сумма, канал);
- при наличии возможности - временное ограничение/приостановка операции и проведение проверки;
- информирование клиента о статусе рассмотрения и итоговом решении в сроки, установленные внутренними документами МФО и договорными условиями.

Процедура 4. Проведение внутренних расследований по подозрительным операциям

Внутреннее расследование проводится при выявлении подозрительной операции по индикаторам, поступлении обращения клиента, совпадении с данными Антифрод-центра и/или при иной обоснованной информации о возможном мошенничестве.

1. Этапы расследования:
2. фиксация события и первичная мера реагирования (приостановка/блокировка/ограничение) при наличии технической возможности;
3. сбор доказательственной базы (логи, устройства, IP/гео, таймлайн действий, документы, записи звонков, переписка);
4. уточнение обстоятельств у клиента (по скрипту), при необходимости - запрос дополнительных документов/подтверждений;
5. анализ и вывод о наличии/отсутствии признаков мошенничества;
6. принятие решения: снятие ограничений либо регистрация инцидента/эскалация и реализация мер.

Результаты расследования оформляются Отчетом внутреннего расследования (Приложение 4).

Процедура 5. Сбор и хранение сведений о реализации существенных рисков мошенничества

МФО обеспечивает сбор и хранение сведений по существенным рискам и инцидентам мошенничества, включая журналы событий, карточки инцидентов, материалы расследований и подтверждающие документы.

- Требования к хранению:
- хранение в защищенных информационных системах/архивах с разграничением доступа по ролям;
- обязательное журналирование действий пользователей и неизменяемость ключевых логов;
- резервное копирование и восстановление;
- сроки хранения - не менее сроков, установленных законодательством РК и внутренними политиками МФО (ИБ, ПДн, архивное хранение).

Процедура 6. Формирование реестра рисков, включающего риски мошенничества

МФО ведет Реестр рисков, который включает отдельный раздел/срез по рискам мошенничества. Форма Реестра приведена в Приложении 5.

Реестр рисков актуализируется владельцем процесса и службой риск-менеджмента/комплаенс не реже одного раза в квартал и внепланово при существенных изменениях.

Процедура 7. Разработка мер минимизации рисков мошенничества

По каждому риску мошенничества разрабатываются меры минимизации (организационные, технические, правовые) и назначаются ответственные за их внедрение и контроль. План обработки рисков оформляется по форме Приложения 6.

- Меры минимизации включают, в том числе:
- настройку антифрод-правил и порогов (скоринг, device/IP/гео, поведенческие факторы, лимиты);
- проверки по источникам/данным Антифрод-центра до осуществления операции и (при необходимости) временное ограничение операции;
- процедуры информирования клиента и подтверждения намерения совершить операцию;
- регистрацию инцидентов и обмен данными с Антифрод-центром через WEB/API;
- меры по требованиям пункта 9-1 применимого НПА (информирование клиента и уполномоченного органа при неправомерных действиях, устранение последствий, исполнение решений правоохранительных органов/судов).

Процедура 8. Мониторинг исполнения мер по обработке рисков мошенничества

МФО осуществляет регулярный мониторинг эффективности и исполнения мер минимизации рисков мошенничества, включая анализ KPI и корректирующие действия.

- Рекомендуемые KPI:
- количество срабатываний индикаторов и доля подтвержденных инцидентов;
- доля ложноположительных срабатываний (false positive);

- среднее время обработки/расследования кейса;
- финансовые потери/возвращенные суммы по инцидентам;
- количество и доля жалоб по мошенничеству, повторные обращения;
- стабильность интеграции с Антифрод-центром и полнота передачи данных (при применимости).

Отчетность по мониторингу формируется не реже 1 раза в месяц и рассматривается ответственными лицами; результаты мониторинга являются основанием для пересмотра Каталога индикаторов, Реестра рисков и Плана обработки рисков.

Взаимодействие с Антифрод-центром НБРК

МФО обеспечивает организационные и технические условия для взаимодействия с Антифрод-центром (включая предоставление/управление доступами уполномоченных пользователей, настройку интеграций и соблюдение требований информационной безопасности).

Базовые сервисы Антифрод-центра, используемые МФО (при подключении): доступ к базе инцидентов, базе о попытках, базе о событиях, базе лиц, задействованных в иных противоправных инцидентах, базе скомпрометированных средств электронного платежа, а также доступ к уведомлениям.

Каналы взаимодействия:

- WEB-интерфейс — для ручной работы уполномоченных пользователей;
- API — для автоматизированного обмена данными (при наличии реализованной интеграции и соответствующего допуска).

Общий алгоритм реагирования (в соответствии с внутренними документами МФО и логикой Правил Антифрод-центра):

7. выявление платежной транзакции/операции с признаками мошенничества и приостановка (при наличии технической возможности);
8. проведение предметного (детального) анализа в сроки, установленные внутренними документами МФО, включая получение (при необходимости) дополнительной информации от клиента для выяснения обстоятельств и принятия решения;
9. при отсутствии оснований (подозрений) — снятие ограничений с последующих транзакций/операций;
10. при подтверждении оснований (подозрений) — регистрация/создание сообщения (карточки) в Антифрод-центре посредством WEB (пользователь) и/или API (интеграция) и дальнейшие действия по внутренним процедурам МФО.

Рассмотрение обращений клиента: при поступлении заявления/обращения клиента о подозрительной операции МФО регистрирует обращение, приостанавливает операцию (при наличии возможности) и применяет алгоритм расследования; при подтверждении оснований создается сообщение (карточка) в Антифрод-центре.

Совпадения с базами событий/попыток: при получении уведомления и/или при выявлении совпадений с данными Антифрод-центра до осуществления платежа/перевода денег МФО применяет установленные меры реагирования (приостановка/блокировка средств, уточнение бенефициара/оснований, информирование клиента) и документирует действия.

Требования по защите данных и конфиденциальности: МФО обязуется использовать доступ к Антифрод-центру исключительно для целей, предусмотренных договором присоединения и Правилами, соблюдать процедуры обеспечения информационной безопасности, обеспечить безопасность данных, полученных посредством системы Антифрод-центра, и принимать меры по защите банковской тайны и персональных данных.

Если техническая интеграция/обмен данными реализуются через поставщика SaaS-платформы (технического оператора), МФО обеспечивает включение в договор с таким поставщиком обязательных условий: (i) запрет самостоятельных решений по клиентам и операциям; (ii) выполнение требований ИБ/ПДн МФО; (iii) журналирование и хранение логов; (iv) уведомление МФО о инцидентах ИБ/компрометации; (v) аудит/право проверок; (vi) запрет субподрядчиков без согласия МФО; (vii) порядок возврата/уничтожения данных; (viii) SLA по доступности и срокам реакции. Ответственность перед клиентами и регулятором за соблюдение законодательства и сохранность персональных данных несет МФО.

Контроль, обучение и пересмотр документа

Контроль исполнения настоящего документа возлагается на владельца процесса и службу комплаенс/риск-менеджмента. Персонал, задействованный в процессах (колл-центр, операции, ИТ/ИБ), проходит первичное и ежегодное обучение по процедурам антифрод и обработке обращений.

Настоящий документ пересматривается не реже одного раза в год, а также при изменении законодательства, требований Антифрод-центра, внедрении новых продуктов/каналов или по итогам существенных инцидентов.

Заключительные положения

Настоящий документ вступает в силу с даты, указанной в Карточке документа, и обязателен для исполнения всеми работниками и подразделениями МФО в части, относящейся к их функциям.

Приложения (формы и шаблоны)

Приложение 1. Каталог индикаторов раннего обнаружения (шаблон)

ID	Индикатор	Описание/условие	Порог/триггер	Уровень риска	Действие (реакция)	Владелец

Приложение 2. Методика оценки вероятности и последствий (шаблон)

Шкалы:

- Вероятность (P): 1 - крайне низкая … 5 - крайне высокая
- Последствия (I): 1 - несущественные … 5 - критические

Матрица риска (P x I):

	I=1	**I=2**	**I=3**	**I=4**	**I=5**
P=1	1	2	3	4	5
P=2	2	4	6	8	10
P=3	3	6	9	12	15
P=4	4	8	12	16	20
P=5	5	10	15	20	25

Приложение 3. Журнал обращений клиентов по мошенничеству (шаблон)

№	**Дата/время**	**ФИО/ ИИН**	**Контакты**	**Канал обращения**	**Суть обращения**	**Операция/ сумма**	**Принятые меры**	**Статус**	**Ответственный**

Приложение 4. Отчет внутреннего расследования (шаблон)

1. Номер кейса / дата начала расследования:

_____

2. Основание (индикатор/жалоба/данные Антифрод-центра):

_____

3. Описание операции/события (сумма, дата, канал):

_____

4. Собранные материалы (логи, документы, записи):

_____

5. Действия МФО (приостановка/блокировка/уведомления):

_____

6. Результат проверки клиента (подтверждение намерения/отрицание):

_____

7. Вывод (признаки мошенничества подтверждены/не подтверждены):

_____

8. Принятое решение (снятие ограничений/регистрация инцидента/эскалация):

_____

9. Корректирующие меры (изменение правил/обучение/доработка):

_____

10. Подписи ответственных лиц:

_____

Приложение 5. Реестр рисков мошенничества (шаблон)

ID риска	Описание	Процесс/канал	Индикаторы	P	I	Уровень	Меры контроля	Остаточный риск	Дата пересмотра/статус

Приложение 6. План обработки рисков мошенничества (шаблон)

ID риска	Мера (контроль)	Тип (орг/тех/прав)	Срок внедрения	Ответственный	Ресурсы	KPI/критерий	Статус

Приложение 7. RACI-матрица (шаблон)

Процесс/задача	Комплаенс/риск	ИБ	ИТ	Операции	Контакт-центр

Обозначения: R - Responsible (исполняет), A - Accountable (несет ответственность за результат), C - Consulted (консультирует), I - Informed (информируется).

Приложение 8. Алгоритм взаимодействия с Антифрод-центром (WEB/API)

Настоящее приложение описывает рекомендуемый минимальный алгоритм действий МФО при выявлении операций с признаками мошенничества и/или при получении уведомлений/совпадений по базам Антифрод-центра. Алгоритм применяется с учетом внутренних сроков и регламентов МФО.

Этап	Триггер/событие	Действия МФО	Ответственный	Фиксация/где
1	Срабатывание индикатора / совпадение с базами Антифрод-центра	Приостановить/ограничить операцию (если технически возможно); зафиксировать параметры операции; инициировать проверку.	Операционный блок / владелец процесса	Логи АИС; карточка кейса; журнал инцидентов
2	Подозрительная операция подтверждается обстоятельствами	Провести предметный анализ; запросить у клиента доп. информацию (при необходимости); проверить реквизиты, устройство, историю, поведение.	Владелец процесса + ИБ/ИТ	Отчет внутреннего расследования; прикрепленные доказательства
3	Нет оснований/подозрений	Снять ограничения; закрыть кейс; отметить причину false positive; при необходимости скорректировать индикатор.	Владелец процесса	Закрытие кейса; запись в журнале
4	Есть основания/подозрения	Создать сообщение/карточку инцидента в Антифрод-центре через WEB или API; продолжить расследование по внутренней процедуре; при необходимости	Уполномоченный пользователь + владелец процесса	WEB/API; регистрационный номер; отчет

		эскалировать в правоохранительные органы.		
5	Обращение клиента (жалоба/заявление)	Зарегистрировать обращение; приостановить операцию (если возможно); применить шаги 2–4; информировать клиента о статусе.	Контакт-центр + владелец процесса	Журнал обращений; шаблоны уведомлений
6	Инцидент закрыт/урегулирован	Собрать и сохранить материалы; обновить реестр рисков; оценить ущерб; сформировать корректирующие меры и KPI.	Владелец процесса + риск/комплаенс	Реестр рисков; план мер; отчет руководству