Simbank

УТВЕРЖДЕНО
Правлением
ОАО «Дос-Кредобанк»
(протокол от «25» июля 2024 г. №39)

Правила
безопасного использования
банковскими платежными картами Visa «Simbank» ОАО «Дос-Кредобанк»

Аннулирование карты — признание карты недействительной и ее изъятие из обращения.

OTP – One Time Password (одноразовый пароль).

Банк – Открытое акционерное общество «Дос-Кредобанк».

Банк-эмитент — банк, участник платежной системы, выпускающий карты, а также отвечающий по обязательствам перед другими банками — участниками платежной системы.

Банк-эквайер — банк, получивший разрешение на осуществление эквайринга, владелец сети периферийных устройств. Обеспечивает проведение авторизаций или транзакций через свои периферийные устройства в соответствии с технологией и нормативными актами соответствующих платежных систем и законодательством Кыргызской Республики.

Банковский счет (далее карт-счет) — счет, открываемый банком держателю карты для движения денежных средств и осуществления транзакций по карте.

Банкомат — аппарат для выдачи и приема наличных денег, внесения денежных средств на карту, получения информации по совершенным транзакциям, осуществления безналичных платежей и получения карт-чека по всем видам транзакций. Банкомат предназначен для самостоятельных операций с картой без участия работников банка. Далее может встречаться как АТМ – Automatic Teller Machine.

Блокирование карты — полный или временный запрет на осуществление операций по карте.

Банкоматная выписка — выписка по карт-счету, формируемая банкоматом по запросу держателя карты. Выписка из банкомата охватывает максимум 10 (десять) последних транзакций, проведенных по карт-счету.

Банковская платежная карта — (далее по тексту карта) платежный инструмент для оплаты товаров, работ и услуг, переводов и проведения иных платежей, а также для получения наличных денег. Карта действительна только в течение срока, указанного на ней. По просроченным картам операции не проводятся.

Держатель карты — физическое лицо, имеющее право пользоваться картой в соответствии с условиями договора банковского обслуживания.

Лимит(ы) — ограничения, установленные банком на максимальную сумму операций по карте. Лимит(ы) могут устанавливаться как на сумму и валюту одной операции, так и на сумму всех операций, проведенных в течение определенного времени.

Мошенническая операция — операция по карте, не санкционированная и не подтвержденная держателем карты.

Нештатная ситуация — ситуация, которая не может быть решена встроенными автоматическими средствами платежной системы и требует специально организованной деятельности персонала.

ПИН-код — персональный идентификационный номер, секретный код для пользования картой. Держатель карты сам устанавливает ПИН-код в приложении «Simbank». ПИН-код состоит из четырех цифр.

Подозрительная операция (сделка) - операция (сделка), подпадающая под следующие признаки:
а) если имеются подозрение или достаточные основания подозревать, что средства являются доходом, полученным преступным путем, в том числе от предикатных преступлений, или связаны с легализацией (отмыванием) преступных доходов;
б) если имеются подозрение или достаточные основания подозревать, что средства связаны с финансированием:
- террористов и экстремистов;
- террористических и экстремистских организаций (групп);
- террористической и экстремистской деятельности.

ПОС-терминал — устройство для приема платежей за товары и услуги в торгово-сервисных предприятиях с использованием карты или инструментов дистанционных платежей.
ПФТД/ЛПД - Противодействие финансированию террористической деятельности и легализации (отмыванию) преступных доходов – комплекс мер, направленных на противодействие финансированию террористической деятельности и легализации (отмыванию) преступных доходов, а также на противодействие финансированию экстремистской деятельности и финансированию распространения оружия массового уничтожения.

Стоп-лист — список карт, которые банк-эмитент запретил принимать в качестве средств платежа.

Выписка по счету — отчет об остатке денежных средств на карт-счете, о движениях денежных средств по карт-счету и операциях по карте за указанный период.

Транзакция — операция по карте (покупка товаров или услуг, обмен валют или снятие наличных), в результате которой происходит дебетование или кредитование карт-счета на сумму транзакции.

Технический овердрафт — задолженность, возникающая, когда сумма расходных операций превышает доступный остаток на карт-счете.

CVV2-код — трехзначный код для проверки подлинности карты при оплате через Интернет и других видах операций. Его можно найти на обратной стороне карты.

3D Secure — современная технология для обеспечения безопасности платежей по картам в Интернете. Позволяет дополнительно идентифицировать держателя карты путем ввода 3D Secure пароля и максимально снизить риск мошенничества.

1. Общие положения

1.1. Правоотношения между держателем карты и Банком по выпуску и обслуживанию карт регулируются Договором публичной оферты о предоставлении банковских услуг физическим лицам (далее по тексту – Договор).
1.2. Передача карты другим лицам в пользование или в качестве залога запрещается. Карта, предъявленная неуполномоченным лицом, подлежит изъятию.
1.3. Карта является собственностью Банка, по истечении срока действия карты, Договора или по первому требованию Банка, карта должна быть в обязательном порядке возвращена в Банк.
1.4. Настоящие правила и тарифы размещаются на официальном сайте Simbank.kg
1.5. Банк вправе в одностороннем порядке изменять настоящие правила, разместив новую редакцию на официальном сайте.

1.6. Банк вправе предоставлять информацию в налоговые органы США по налоговым резидентам США в рамках требований закона FATCA

2. Пользование ПИН-кодом

2.1. После получения карты держатель карты активирует ее в мобильном приложении «Simbank» путем ввода последних 8 цифр карты.

2.2. После успешной активации карты в мобильном приложении «Simbank» ПИН-код карты будет идентичным с мобильным приложением.

2.3. Смена ПИН-кода осуществляется держателем карты в мобильном приложении банка.

2.4. Держатель карты самостоятельно выбирает комбинацию из 4 цифр для ПИН-кода. Держатель карты не должен использовать очевидные, легко предполагаемые цифровые комбинации, например, последние цифры номера телефона, дату рождения и пр.

2.5. При наборе ПИН-кода цифры на дисплеях электронных устройств специально не высвечиваются, а заменяются условным знаком. Важно не допускать ошибок при наборе. Если три раза подряд (с любым временным промежутком) набирался неправильный ПИН-код, карта автоматически блокируется. Клиенту необходимо обратиться в службу поддержки Банка, по номеру телефона 7700, который указан на карте.

2.6. Карточные операции, подтвержденные ПИН-кодом, банк воспринимает как совершенные держателем карты.

3. Применение карты.

Карту можно использовать для:

- Оплаты товаров и услуг в безналичной форме в торгово-сервисных предприятиях.
- Получения наличных денег в банковских отделениях и через банкоматы.
- Проведения операций в сети Интернет.

4. Оплата картой в торгово-сервисных предприятиях.

4.1. Все пункты, в которых обслуживаются карты, оснащены информационными указателями с логотипами ПС VISA.

4.2. Чтобы расплатиться за товары или услуги, необходимо предъявить работнику торговой точки карту/поднести к ПОС-терминалу.

4.3. В целях безопасности и защиты персональных данных все транзакции с использованием карт в торгово-сервисных предприятиях должны проводиться в присутствии держателя карты.

4.4. В некоторых торговых и сервисных организациях при крупных покупках могут попросить удостоверение личности. Поэтому при оплате картой банк настоятельно рекомендует иметь при себе паспорт или другой документ, удостоверяющий личность.

4.5. Авторизация при оплате картой осуществляется с помощью ПОС-терминала. Кассир набирает на клавиатуре сумму операции. Затем кассир (или сам держатель карты) помещает карту в считывающее устройство ПОС-терминала или подносит карту к бесконтактному чип-ридеру на ПОС-терминале. Запрос поступает в банк по каналам связи. Если держатель карты набрал правильный ПИН-код и на карте достаточно денег, распечатывается чек в двух экземплярах, подтверждающий совершение транзакции. Держателю карты выдается один экземпляр чека. Необходимо проверить данные в чеке. В зависимости от принятой технологии распечатанный чек может заверяться подписями держателя карты и кассира.

4.6. Запрещается подписывать чек, если на нем не прописана сумма операции, которая будет списана с карты, отсутствует дата (или другие детали операции). Если держатель карты обнаружит неточности в указанной информации, нужно отказаться от подписи и попросить отмену операции и чек об отмене.

4.7. Банк настоятельно рекомендует сохранять чеки после покупок. Они могут пригодиться в случае спорных вопросов и неточностей при списании средств с карт-счета.

5. Оплата картой в сети Интернет.

5.1. Для оплаты картой в Интернете используются ее реквизиты: номер карты, срок действия, имя держателя карты. Некоторые сайты могут дополнительно запрашивать такие реквизиты, как CVV2 и 3D Secure пароль.

5.2. Доступ к 3D Secure и оплате в Интернете открыт по умолчанию для всех карт VISA.

5.3. Ответственность за возможные риски, например, проведение несанкционированных интернет-платежей по карте третьими лицами, возлагается на держателя карты. При этом банк принимает заявления от держателя карты (на возврат денежных средств и/или претензионную работу по таким операциям) и обрабатывает согласно действующим правилам МПС.

5.4. Код CVV2 — это трехзначный код, который печатается на оборотной стороне карты.

5.5. Банк рекомендует совершать покупки только на проверенных сайтах известных компаний.

5.6. Также банк рекомендует проводить платежи на сайтах, поддерживающих технологию безопасности 3D Secure.

5.7. При проведении операции по технологии 3D Secure держателю карты нужно ввести пароль, который приходит в СМС на номер, указанный им при выпуске карты/в push-уведомлении, этот пароль является одноразовым.

5.8. Для безопасных операций в сети Интернет держателю карты необходимо:

- Своевременно обновлять свой браузер и антивирусные программы.
- Проверить срок действия карты, отсутствие блокировки и т.д.
- Убедиться, что на карте достаточно денег для совершения платежа.
- Воздержаться от совершения операций на автоматически перенаправленных страницах или во всплывающих окнах.
- Для проведения оплаты и подтверждения заказа четко следовать указаниям сайта.

5.9. Возможные причины отказа в проведении платежа:

- На карте недостаточно средств.
- По карте запрещены платежи в сети Интернет или установлены иные ограничения.
- Истек срок действия карты.
- Держатель карты не указал 3D Secure пароль.
- Карта заблокирована.
- Банком введен запрет на проведение подозрительных операций.
- При открытии карты был указан неверный/утраченный номер телефона и сообщение с кодом 3D Secure приходит на неверный номер.
- Сайт или страна находится под санкциями и считаются высоко рискованными.
- Не разрешены браузерами cookie.

  Для выяснения причин отказа держатель карты может обратиться в банк.

5.10. Для полной или частичной отмены платежа держателю карты необходимо обратиться в службу поддержки Интернет-магазина.

5.11. Держатель карты может самостоятельно заблокировать проведение платежей по карте через Интернет. Для этого необходимо в приложении Simbank в разделе «Лимиты» поставить лимит 0 (ноль).

6. Получение наличных денег в банкомате.

6.1. Перед использованием банкомата необходимо осмотреть его на наличие подозрительных устройств: неровно установленной клавиатуры, накладок над экраном

банкомата и т.д. При обнаружении такого устройства нужно воздержаться от проведения операций в банкомате и по возможности сообщить о своих подозрениях сотрудникам банка по телефону, указанному на банкомате, или позвонив в Колл-центр Банка.

6.2. Для получения наличных денег в банкомате держатель карты вводит ПИН-код и следует инструкциям на экране банкомата.

6.3. Отменить операцию можно с помощью кнопки «Отмена» / «Cancel».

6.4. При наборе ПИН-кода нужно убедиться, что его не видят посторонние. Если трижды ввести неправильный ПИН-код, карта будет заблокирована. Для разблокировки карты следует обратиться в службу поддержки банка по номеру 7700 или в мессенджерах Telegram, WhatsApp.

6.5. В целях безопасности все операции в банкомате следует совершать самостоятельно, без помощи третьих лиц.

6.6. В банкоматах разных банков одноразовый лимит для снятия наличных может отличаться.

6.7. Рекомендуем сохранять получаемые через банкомат квитанции, так как они заверены ПИН-кодом и являются подтверждением сделки.

6.8. После появления на экране надписи «Заберите свою карту» нужно немедленно забрать карту, в противном случае она будет изъята банкоматом.

6.9. Выданные банкоматом деньги необходимо забрать в течение 20 (двадцати) секунд, иначе сработает система защиты и банкомат заберет их назад. Это предусмотрено в целях безопасности.

6.10. Если банкомат изъял карту или деньги, не стоит сразу уходить, нужно подождать какое-то время. Возможно, это был технический сбой и банкомат вернет карту или деньги, а держателя карты уже не будет рядом.

6.11. Возможные причины отмены операций в банкомате:

- В банкомате нет подходящих банкнот для запрашиваемой суммы. Следует запрашивать сумму, кратную минимальному номиналу банкнот, указанному в банкомате.
- Запрашиваемая сумма превышает лимит разовой выдачи, определяемый габаритами банкомата. Можно разделить запрашиваемую сумму на части и повторить операцию несколько раз.
- Запрашиваемая сумма превышает остаток денег на карте. Чтобы узнать остаток на карте, можно использовать такую опцию в меню банкомата.
- При снятии наличных в банкомате убедитесь, что банкомат обслуживает карты нужной платежной системы (обычно на банкоматах располагаются логотипы платежных систем, которые обслуживаются банкоматом).

7. При утере/краже карты.

7.1. В случае утери или кражи карты, также если имеются подозрения использования карты неуполномоченным лицом, необходимо срочно обратиться в банк, оператор банка моментально заблокирует карту, либо держатель карты может самостоятельно заблокировать карту через приложение банка. При этом после блокировки держатель карты все еще сможет совершать платежи в приложении Simbank и покупки через Google Pay/Garmin Pay.

7.2. В случае утери или кражи карты, а также смартфона с аккаунтом Simbank, держатель карты должен заблокировать карту, обратившись в поддержку банка: по номеру 7700 или в мессенджерах Telegram, WhatsApp.

7.3. Держатель карты несет ответственность за карточные операции, осуществленные до блокировки карты, и освобождается от нее с момента блокировки.

7.4. Если после заявления о потере или краже карты держатель ее найдет, необходимо уведомить об этом банк. Если держатель захочет далее пользоваться этой картой, ему нужно обратиться в банк для разблокировки карты.

7.5. Банк настоятельно рекомендует проверять выписку по карт-счету в последующие месяцы, чтобы убедиться, что по карте не были проведены несанкционированные транзакции.

8. Нештатные ситуации в платежной системе.

8.1. В платежной системе могут возникнуть следующие нештатные ситуации: перебои энергоснабжения; сбои каналов связи; сбои аппаратного и программного обеспечения системы; форс-мажорные обстоятельства (пожар, наводнение, землетрясение и т.д.).

8.2. Банк принимает все возможные меры для обеспечения бесперебойной работы оборудования и систем, участвующих в карточных операциях.

9. Подозрительные операции по карте.

9.1. Если Банк подозревает, что с картой совершаются мошеннические (нехарактерные), подозрительные действия, он вправе запросить дополнительную информацию и документы у держателя карты. В случае не предоставления держателем карты в установленный срок запрошенных документов, информации, либо если предоставлены недостоверные документы Банк имеет право отклонить операцию и/или заблокировать карту, с последующим закрытием карт-счета

9.2. Банк имеет право заблокировать/отклонить операции, проводимые на запрещённых сайтах, сайтах, представляющие нелегальные услуги/товары, операции по онлайн-казино, на букмекерских сайтах, на сайтах, содержащий контент для взрослых и прочие платежи, в рамках законодательства Кыргызской Республики по противодействию финансированию террористической деятельности и легализации (отмыванию) преступных доходов (далее по тексту - ПФТД).

9.3. Держатель карты не должен проводить операции, запрещенные законодательством Кыргызской Республики и операции, подпадающие под Закон Кыргызской Республики о ПФТД/ЛПД.

9.4. Банк имеет право проводить мониторинг мошеннических и подозрительных операций, требовать у держателя карты документы, необходимые для проведения операций по счету, подтверждающие законность и экономическую целесообразность совершаемой операции, и действительность осуществления клиентом реальной экономической деятельности.

9.5. Если держатель карты обнаружил спорную операцию в выписке по карт-счету, ему необходимо обратиться к сотруднику банка для уточнения деталей. В случае несанкционированного использования денег на карте держателю карты необходимо подать претензионное заявление на возврат средств. Для этого можно обратиться в службу поддержки банка: по номеру 7700 или в мессенджерах Telegram, WhatsApp.

9.6. Держатель карты может подать претензионное заявление в течение 45 (сорока пяти) календарных дней с момента совершения операции. По истечению этого срока банк имеет право не принимать заявление.

9.7. Решение спорных ситуаций происходит следующим образом: банк проводит расследование по претензионной операции. При этом банк имеет право запросить дополнительные документы (чек об оплате, чек о снятии денег в АТМ), подтверждающие совершение операции. Если подтверждается, что деньги были списаны некорректно и не по вине держателя карты, банк возвращает средства на карту. Рассмотрение претензии и принятие решения может занимать до 3 (Трех) месяцев.

10. Правила безопасности и борьбы с мошенничеством.

10.1. Банк не несет ответственности за возникшие убытки держателя карты, в связи несоблюдением им правил безопасности по использованию карты.
10.2. Запрещено передавать карту третьему лицу. Использование карты третьим лицом банк воспринимает как грубое нарушение. Это может повлечь за собой расторжение договора по инициативе банка.
10.3. Храните карту в укромном месте. Не стоит оставлять карту в местах, где кто-то сможет ею воспользоваться или скопировать реквизиты (номер карты, образец подписи, CVV-код и другие данные).
10.4. Чтобы не испортить магнитную полосу, не держите карту рядом с источниками электромагнитного излучения (сотовые телефоны, телевизоры, СВЧ-печи, аудио- и видеоаппаратура и т.п.). Будьте осторожны при расчетах в местах, где используется магнитная кодировка товаров — это может привести к отказу в обработке или неправильной обработке карты в банкоматах и ПОС-терминалах.
10.5. Не сообщайте ПИН-код карты третьим лицам. Операции, проведенные с вводом ПИН-кода, признаются как совершенные держателем карты и оспариванию не подлежат.
10.6. Не записывайте ПИН-код на саму карту или в документы, хранящиеся рядом с картой.
10.7. При совершении покупки не теряйте карту из виду. Заберите карту сразу же после завершения транзакции.
10.8. Все операции с картой в торговых точках должны проводиться в присутствии держателя карты.
10.9. Перед проведением операции в банкомате проверьте, нет ли внешних признаков его неисправности. Обнаружив рядом с банкоматом или на нем посторонние или подозрительные устройства, сообщите об этом в банк, обслуживающий банкомат, затем воспользуйтесь другим банкоматом.
10.10. Не рекомендуется пользоваться теми банкоматами, на экране которых отображается сообщение с просьбой о переходе на другие банкоматы. Банки не размещают подобные сообщения.
10.11. Выбирайте банкоматы в хорошо освещенных и удобных местах. Убедитесь, что при совершении транзакции рядом с вами нет посторонних лиц.
10.12. Рекомендуется хранить все чеки, для последующего контроля расходов, и не выбрасывать чеки в контейнер для мусора в публичном месте.
10.13. Нельзя вводить реквизиты карты на подозрительных сайтах. В противном случае вы рискуете, что ваши деньги будут похищены.
10.14. При вводе ПИН-кода убедитесь, что его не видели посторонние.
10.15. Банк всегда оповещает держателя карты о всех транзакциях по карте с помощью Push-уведомлений в приложении Simbank.
10.16. Своевременно обновляйте контактные данные, которые вы предоставили банку. Так банк всегда сможет связаться с вами в случае подозрительной операции по карте.
10.17. Соблюдайте правила безопасности в интернете. Не переходите по ссылкам, присланным в подозрительных или непонятных сообщениях на электронную почту или в социальных сетях. Не передавайте 3D Secure пароли третьим лицам.
10.18. Не загружайте подозрительные файлы из электронной почты, которых вы не ожидали.
10.19. Никому не сообщайте свои пароли и персональные данные — будь то по телефону, лично или в переписке.
10.20. Внимательно анализируйте адреса сайтов (URL), на которые вас переадресовывают. Часто бывает, что мошеннический сайт выглядит идентично настоящему, при этом URL-адрес отличается от оригинального (например, заканчиваться на com. вместо.gov).
10.21. Своевременно обновляйте свой браузер и программы безопасности.

11. Ограничения по картам.

11.1. В целях безопасности банк вправе устанавливать ограничения на карточные операции. Величина лимитов, а также условия, сроки и порядок их установления, банк определяет самостоятельно.

11.2. Банк имеет право установить ограничения на карточные операции в рамках противодействия мошенничества и ФТД/ЛПД, если:

11.3. Данные держателя карты или кого-либо из участников операции указаны в действующих списках физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об их участии в террористической и экстремистской деятельности, распространении оружия массового уничтожения и легализации (отмывании) преступных доходов и в иных противоправных действиях;

11.4. Держатель карты или кто-либо из участников операции зарегистрирован в высоко рискованной стране (государство/территория), не соблюдающей рекомендации ФАТФ, и/или предоставляющей льготный налоговый режим и/или не предусматривающей полное раскрытие и представление информации при проведении финансовых операций, либо в отношении которой действуют международные санкции.

11.5. Стандартные ограничения, установленные банком, могут быть изменены по письменному обращению держателя карты в банк.

11.6. Также банк может установить ограничение на сумму бесконтактных платежей по карте (NFC), которые не подтверждаются ПИН-кодом.

12. Срок действия карты и расторжение договора.

12.1. Срок действия карты (месяц и год) указаны на самой карте. Карта действительна до последнего дня, указанного на ней месяца включительно. Все просроченные карты блокируются и подлежат сдаче в банк.

12.2. Держатель карты вправе закрыть карту и расторгнуть договор в одностороннем порядке, подав заявление на аннулирование карты.

12.3. Банк вправе блокировать/аннулировать карту и расторгнуть договор с держателем карты при невыполнении им условий и правил договора.

12.4. При расторжении договора держатель карты должен погасить имеющуюся задолженность и сдать карту.

12.5. При расторжении договора по инициативе любой из сторон комиссия за годовое обслуживание и иные уплаченные держателем карты комиссии не возвращаются.

12.6. Остаток денежных средств по карт-счету выдается держателю карты при отсутствии задолженности перед банком.

13. Прочие условия.

13.1. Держатель карты обязан в течение 5 (Пяти) дней извещать банк обо всех изменениях в данных, которые он указал в документах при оформлении карты. Если держатель карты этого не делает, банк не несет ответственность за последствия, которые могут возникнуть.