ПРАВИЛА ПОЛЬЗОВАНИЯ БАНКОВСКИМИ ПЛАТЕЖНЫМИ КАРТАМИ

Внимательно ознакомьтесь с Правилами и обязательно сохраните до окончания срока действия выданной Вам банковской платежной карты

1. Термины и определения.

Авторизация	Разрешение Банка-эмитента на осуществление банковских операций с использованием Банковской платежной карты.
Аннулирование карты	Признание карты недействительной и изъятие ее из обращения.
Банк-Эмитент	Банк, являющийся участником платежной системы, выпускающий (эмитирующий) карты, а также отвечающий по обязательствам перед другими банками – участниками платежной системы.
Банк-Эквайер	Банк, получивший разрешение на осуществление эквайринга, владелец сети периферийных устройств, обеспечивающий возможность проведения 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 Держателя карты.
Банкомат	Аппаратно-программный комплекс для выдачи и приема наличных денежных средств, записи денежных средств на карту, получения информации по совершенным транзакциям держателем карты, осуществления безналичных платежей и выдачи карт-чека по всем видам произведенных транзакций. Банкомат предназначен для самостоятельного совершения держателем операций с использованием карты без участия уполномоченного работника Банка. Далее может встречаться как АТМ – Automatic Teller Machine.
Блокирование карты	Полный или временный запрет на осуществление операций с использованием карты.
Банкоматная выписка	Выписка по карт-счету, формируемая банкоматом по запросу Держателя карты. Выписка из банкомата охватывает максимум 10 (Десять) последних транзакций, произведенных по карт-счету Держателя карты.
Банковская Платежная Карта (далее по тексту карта)	Платежный инструмент, предназначенный для оплаты товаров, работ и услуг, переводов и проведения иных платежей, а также для получения наличных денежных средств в пределах остатка денежных средств, имеющихся на карт-счете. Карта действительна только в течение срока, указанного на ней. По просроченным картам операции не производятся.
Виртуальная карта	специальная карта, выпускаемая в электронном виде без физического носителя.
Держатель карты (картодержатель)	Физическое лицо, в том числе уполномоченное юридическим лицом/индивидуальным предпринимателем-владельцем счета, имеющий/ее право совершать операции с использованием карты на основании заключенного договора с эмитентом.
Дополнительная карта	Карта, оформленная по карт-счету на доверенное лицо Держателя. Держатель вправе установить лимит на сумму денег карточных операций по дополнительной карте.
Задолженность	Все суммы, которые Держатель должен уплатить Банку в связи с выпуском/перевыпуском карты/дополнительной карты, открытием, обслуживанием (ведением), проведением карточных операций, закрытием карт-счета, техническим овердрафтом, а также иных сумм, подлежащих оплате согласно тарифам Банка.
Банковская платежная карта (карта)	платежный инструмент, используемый при проведении расчетов при покупке товаров, услуг, получении наличных денег в национальной и иностранной валютах, осуществлении денежных переводов, а также для расчетов в форме электронных денег через терминалы, банкоматы или иные устройства (периферийные устройства).
Кодовое слово	Слово (либо комбинация символов), указанное Держателем в Заявлении-анкете на выпуск карты, по которому Банком может идентифицировать Держателя карты и предоставить информация о состоянии карт-счета и карт по телефону.

Лимит(ы) денежных средств	Установленные Банком лимиты по максимальной сумме, производимые посредством карты. Лимит(ы) могут устанавливаться как на сумму и валюту одной операции, так и на сумму всех операций, произведенных в течение определенного времени.
Мошенническая операция	Операция по банковской платежной карте не санкционированная и не подтвержденная Держателем карты.
Неснижаемый остаток	Сумма денежных средств, определяемая Банком, которая не подлежит авторизации и являющаяся залогом Держателя перед Банком.
Нештатная ситуация	Ситуация, которая не может быть решена встроенными автоматическими средствами управления рисками отдельной платежной системы в соответствии с правилами и технологией работы системы и требует для ее разрешения специально организованной деятельности персонала оператора или участника данной платежной системы.
PIN-код	Персональный идентификационный номер, позволяющий аутентифицировать пользователя для совершения операции, т.е. секретный код, присваиваемый каждой карте и предназначенный для идентификации такого Держателя карты. PIN-код состоит из последовательности четырех цифр.
ПВН	Пункт выдачи наличных.
POS-терминал	Это электронное расчетное устройство, установленное в отделениях Банка для снятия наличных, в торгово-сервисных предприятиях, используемое при проведении карточной операции Держателя карты по оплате за товары и услуги посредством карты.
ТСП	Торгово-сервисное предприятие с наличием POS-терминала для принятия и обслуживания карт.
Стоп-лист	Список карт в Платежной системе, запрещенных Банком к приему в качестве средств платежа.
Счет-выписка (далее по тексту выписка)	Отчет об остатке денежных средств на карт-счете Держателя карты, о движениях денежных средств по карт-счету и проведенных операциях посредством карты за указанный период.
Транзакция	Операция с использованием карты при покупке товаров, услуг, обмена валют или получения наличных денежных средств, в результате которой происходит дебетование или кредитование карт-счета на сумму транзакции.
Технический овердрафт	Задолженность, возникающая вследствие превышения суммы выплат (расходных операций) над доступным остатком средств на карт-счете.
Фишинг	Один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени Банка, популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих, однако на самом деле они являются поддельными. В письмах вас вежливо попросят обновить или подтвердить верность персональной информации, нередко упоминают какие-либо проблемы с данными. Затем вас перенаправляют на поддельный сайт, внешне неотличимый от настоящего, где вас просят ввести учетные данные. Если злоумышленники заполучат необходимую информацию, это может вести к краже персональных данных или средств.
CVV-код (card verification value 2)	Трехзначный код для проверки подлинности карты при оплате через Интернет и других видах операций, нанесенный на обратной стороне карты.
3D Secure	Современная технология обеспечения безопасности платежей по картам в сети интернет, позволяет дополнительно идентифицировать держателя карты путем ввода 3D Secure пароля, и максимально снизить риск мошенничества в Интернете с использованием платежных карт.
Digital Wallet (Apple Pay/Apple Wallet/Google Pay/Google Wallet)	приложение или онлайн-сервис, для безопасного хранения карточных платежных данных, который позволяет оплачивать покупки в магазинах (через NFC), на сайтах и в приложениях через устройства (смартфон/Apple Watch/Garmin/ iPad/Mac), к которому привязывается банковская платежная карта (работает на смартфонах Apple (версии 6 и новее) и Android (версии 4.4 и выше, на которых включена функция NFC).

Google PayСервис провайдер	Сервис, который позволяет оплачивать покупки в магазинах, на сайтах/ приложениях, а также проводить обналичивание бесконтактным способом через смартфон, к которому привязывается карта VISA (работает на телефонах Android версии 4.4 и выше, на которых включена функция NFC). С помощью Google Pay/Garmin Pay картодержатели VISA могут оплачивать покупки в интернет-магазинах, на сайтах и в приложениях, используя аккаунт Google с привязанной к нему банковской картой.
Процессинг	Лицензируемая деятельность, включающая в себя взаимосвязанные процессы по приему, обработке и выдаче участникам платежной системы финансовой информации.
Near Field Communication (NFC)	Технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, и/или картой и устройствами. По требованию большинства платежных систем карты должны поддерживать технологию бесконтактной оплаты (NFC)
QR-код	Двухмерный символ штрих кода для передачи платежных данных, который используется при проведении безналичных платежей и переводов.

2. Общие положения.

2.1. Правила пользования банковскими платежными картами (далее по тексту – Правила) определяют порядок выпуска и обслуживания Банком карт, порядок совершения операций с использованием карт, а также правила по безопасному использованию карт.

2.2. Правоотношения между Держателем и Банком по выпуску и обслуживанию карт регулируются Условиями банковского обслуживания физических лиц ОАО «БАКАЙ БАНК (далее по тексту Договор):

- для индивидуальных предпринимателей (ИП) - Условия банковского обслуживания индивидуальных предпринимателей в ОАО «БАКАЙ БАНК»
- для юридических лиц (ЮЛ) при выпуске корпоративной карты. - ДОГОВОР о выпуске и обслуживании корпоративных карт

2.3. Передача карты другим лицам в пользование или в качестве залога запрещается. Карта, предъявленная неуполномоченным лицом, подлежит изъятию.

2.4. Карта является собственностью Банка, по истечении срока действия карты, Договора, изменения ФИО картодержателя или по первому требованию Банка, карта должна быть в обязательном порядке возвращена в Банк.

2.5. Настоящие Правила и тарифы Банка размещаются на официальном сайте Банка www.bakai.kg.

2.6. Банк вправе в одностороннем порядке изменять настоящие Правила, уведомив о внесении изменений путем размещения информации на официальном интернет сайте Банка по адресу: www.bakai.kg с учетом срока, установленного действующим законодательством Кыргызской Республики.

3. Порядок выдачи карты

3.1. Банк выдает изготовленную карту непосредственно Держателю, либо его доверенному лицу. При получении карты Держатель должен расписаться в специально предусмотренном для этого поле на оборотной стороне карты.

3.2. Карта может выдаваться вместе с PIN-кодом в PIN-конверте, либо PIN-код может присваиваться самим Держателем через мобильное приложение Банка, после аутентификации. В случае присвоения PIN-кода через мобильное приложение Банка для активации PIN-кода необходимо совершить первую финансовую операцию в банкомате с вводом установленного PIN-кода.

3.3. В целях защиты средств на карт-счете Держателя, Банк настоятельно рекомендует не сообщать PIN-код третьим лицам и не хранить его в бумажном виде.

3.4. При получении карты удостоверьтесь, что латинское написание Вашего имени на карте до буквы совпадает с написанием Вашего имени в заграничном паспорте. Иначе у Вас могут возникнуть сложности при оплате покупок за границей.

3.5. Сроки изготовления и выдачи карты, включая стандартный и срочный выпуск, зависят от типа карты и региона получения. Подробную информацию можно уточнить в отделениях Банка или по телефону контакт-центра __6111 (для звонков с мобильных) WhatsApp/Telegram: +996554006111__.

3.6. Банк не производит срочный выпуск карты до полной оплаты комиссии за срочный выпуск согласно тарифам.

3.7. В случае выпуска карты, но неявки Держателя в Банк для получения карты в срок более 6 (шести) месяцев со дня подачи заявления, Банк имеет право аннулировать карту и закрыть карт-счет и не возвращать

Держателю выплаченную им полностью или частично комиссию за ее выпуск и годовое обслуживание согласно установленным тарифам банка.

3.8. Доставка карты за пределы Кыргызской Республики не осуществляется согласно действующему законодательства Кыргызской Республики.

4. Пользование PIN-кодом.

4.1. Держатель карты самостоятельно присваивает PIN-код через мобильное приложение «BAKAI», выбрав необходимую карту, в разделе «Настройки» - Присвоить/Сменить PIN-код. Для активации PIN-кода необходимо совершить любую первую операцию в банкомате с вводом установленного PIN-кода (например, просмотр баланса или снятие наличных средств).

4.2. Смена PIN-кода через мобильное приложение Банка производится согласно п.4.2.

4.3. Комбинация цифр (4 цифры) выбирается по усмотрению Держателя карты. Избегайте очевидных, легко предполагаемых цифровых комбинаций, например, окончание Вашего номера телефона, дата Вашего дня рождения набор одинаковых цифр и прочее,

4.4. При наборе PIN-кода цифры на дисплеях электронных устройств специально не высвечиваются, а заменяются условным знаком. Важно не допускать ошибок при наборе. Если шесть раз подряд (с любым временным промежутком, при пользовании одним или разными электронными устройствами) набирался неправильный PIN-код, карта автоматически блокируется, и она будет задержана банкоматом или может быть изъята в пункте обслуживания до выяснения обстоятельств.

4.5. Карточные операции, подтверждаемые набором PIN-кода, считаются совершенными Держателем карты.

4.6. Не храните PIN-код вместе с картой, не записывайте PIN-код на карте, не сообщайте PIN-код третьим лицам.

5. Применение карты.

- Оплата товаров и услуг в безналичной форме в торгово-сервисных предприятиях, принимающих к оплате карты, включая оплату через QR-коды (ELQR).
- Получение наличных денежных средств в банковских учреждениях и через Банкоматы.
- Проведение операций в сети Интернет, включая оплату товаров, услуг, подписок и сервисов.
- Проведение операций через мобильные приложения и интернет-банкинг.
- Перевод денежных средств с карты на карту, в том числе по номеру карты, номеру телефона или QR-коду.
- Пополнение карточного счета через кассы Банка, платежные терминалы, автоматизированные депозитные машины (АДМ), банкоматы, а также иные каналы, предусмотренные Банком.

6. Процесс оплаты картой в торгово-сервисных предприятиях.

6.1. Все пункты обслуживания карт оснащаются указателями с логотипами платежных систем (например, ЭЛКАРТ/Visa/Mastercard/UPI) для информирования Держателей карт о возможности обслуживания по карте в данном пункте.

6.2. Держатель карты может осуществить оплату за товары или услуги в торгово-сервисном предприятии (ТСП) посредством физической карты. Если карта поддерживает бесконтактную оплату (NFC), достаточно поднести карту к POS-терминалу. Если карта подключена к Digital Wallet, оплату можно произвести с помощью устройств (смартфон/Apple Watch/Garmin/ iPad/Mac). В всех случаях устройство прикладывается к POS-терминалу. Также, возможна оплата посредством сканирования QR-кода POS-терминала через мобильное приложение Банка, если такая функция поддерживается точкой продаж.

6.3. При использовании Держателем карты в устройствах с поддержкой NFC, Банк не несет ответственности за перебои или сбои в работе программного обеспечения или технических систем, обрабатывающих операции с использование токена, если данные сбои произошли не по вине Банка (включая сбои на стороне платёжных сервисов, таких как Apple Pay, Google Pay, Garmin Pay и др.).

6.4. Безналичная оплата с помошью NFC модуля производится в пределах установленного лимита по карте, а также лимита, установленного на POS-терминале банком-эквайером (банком, кому принадлежит POS-терминал)

6.5. Все транзакции с использованием карт или устройств в торгово-сервисных предприятиях должны проводиться в присутствии Держателя карты. Это необходимо в целях снижения риска неправомерного получения персональных данных Держателя, указанных на карте или устройстве.

6.6. В некоторых торгово-сервисных предприятиях при крупных покупках, могут попросить предъявить удостоверение личности. Поэтому при оплате крупной покупки картой или устройством, Банк настоятельно рекомендует иметь при себе паспорт или иной удостоверяющий личность документ.

6.7. Кассир принимает карту или устройство для оплаты и осуществляет авторизацию с помощью POS-терминала. В зависимости от типа карты или устройства оплата может производиться путём:

- введения карты в считывающее устройство (чип-картридер);

– прикладывания карты или устройства к POS-терминалу для бесконтактной оплаты (NFC).

После ввода суммы операции и получения подтверждения авторизации запрос направляется в Банк по защищённым каналам связи. При вводе правильного PIN-кода Держателем карты и наличии достаточного остатка на карте операция подтверждается, и распечатывается чек. Один экземпляр чека передаётся Держателю карты. Рекомендуется проверять корректность данных, указанных в чеке. При бесконтактной оплате ввод PIN-кода не требуется, если сумма операции находится в пределах лимита, установленного банком-эквайером или банком-эмитентом в соответствии с требованиями платёжной системы.

6.8. В случаях, когда при оплате требуется подпись на чеке, рекомендуется внимательно проверять сумму операции и реквизиты до подписания.

6.9. Банк рекомендует сохранять копии чеков, полученных в подтверждение оплаты товаров и услуг, до момента окончательного списания средств с карт-счёта. Чеки могут потребоваться для подтверждения операции в случае возникновения спорных финансовых ситуаций.

6.10. Банк рекомендует проводить оплату картой или устройством только в торгово-сервисных предприятиях, вызывающих доверие. Особую осторожность следует соблюдать при использовании карты за рубежом, особенно в странах и регионах с повышенным уровнем мошеннической активности.

7. Процесс использования карты в сети Интернет.

7.1. Оплата товаров или услуг в сети Интернет с использованием карты или устройства осуществляется без физического предъявления карты или устройства, но с обязательным вводом её реквизитов: номера карты, срока действия карты, а также имени и фамилии Держателя карты (как указано на карте). Дополнительно, для подтверждения операции запрашиваются такие данные, как код CVV2 и пароль 3D Secure, в соответствии с требованиями интернет-ресурса. Для завершения оплаты необходимо ввести все требуемые данные и нажать кнопку «Оплатить».

7.2. По картам доступ к технологии 3D Secure подключается по умолчанию (при обязательном указании номера телефона Держателя карты), что автоматически обеспечивает возможность проведения интернет-операций.

7.3. Операции в сети Интернет производится в пределах установленного лимита по карте, а также лимита, установленного банком-эквайером (владельцем банкоматов и POS-терминалов).

7.4. Вся ответственность за возможные последствия проведения операций через Интернет, в том числе за риск несанкционированных операций третьими лицами по карте, возлагается на Держателя карты. При этом Банк вправе отказать в приёме заявлений о возврате денежных средств и/или претензионной работе по таким операциям.

7.5. Держателю карты важно своевременно проверять на актуальность свои подписки на различных сайтах и приложениях, поскольку при неуспешных авторизациях (при недостаточности средств или отключении интернет платежей) торговая точка/сайт могут направить файл на списание и сумма может быть списана без предварительной авторизации. При этом ответственность за платежи будет нести Держатель карты, так как он сам осуществил подписку и согласился с условиями автоматического списания и будет должен погасить задолженность перед Банком. Если подписка неактуальна или невозможно отключить самостоятельно, необходимо обратиться в Банк.

7.6. Ключевым элементом обеспечения безопасности при проведении платежей в сети Интернет с использованием платежных карт является идентификация Держателя карты. Для осуществления оплаты в сети Интернет – магазине или иным поставщиком услуг в сети Интернет используется код CVV2/CVC2.

7.7. Код CVV2/CVC2 — это трёхзначный код, предназначенный для подтверждения операций в сети Интернет. В зависимости от типа карты код может быть размещён на обратной стороне карты или отображаться в мобильном приложении Банка.

7.8. Банк рекомендует совершать покупки в сети Интернет только на проверенных сайтах известных и надежных компаний.

7.9. Для обеспечения безопасности проведения операций в сети Интернет, Банк рекомендует проводить платежи на сайтах, поддерживающих технологию безопасности 3D Secure. Подключение карт к технологии 3D Secure осуществляется в автоматическом режиме. Статус подключения карты к технологии 3D Secure Держатель карты может уточнить, обратившись в Банк.

7.10. При проведении операции в сети Интернет, поддерживающих технологию 3D Secure Держателю карты предлагается ввести одноразовый пароль (OTP-код), который поступает посредством СМС на мобильный номер телефона или на электронную почту, указанные Держателем карты при открытии карты. СМС-пароль является одноразовым и действителен для совершения только одной операции.

7.11. Перед совершением операции в сети Интернет Держатель карты должен:

– Поддерживать свой браузер обновленным и своевременно устанавливать обновления безопасности.
– Проверить срок действия карты, отсутствие блокировки и иных ограничений.
– Убедиться в наличии достаточных денежных средств на карте для совершения платежа.

- Воздерживаться от совершения операций на автоматически перенаправленных страницах или всплывающих окнах.
- Внимательно следовать инструкциям сайта при оформлении оплаты и подтверждении заказа.

7.12. 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 или вовремя не ввел пароль;
- карта может быть заблокирована;
- возможно банком введен запрет на проведение запрещенных операций с уровнем высокого риска (игорная деятельность, эскорт услуги, и пр.);
- при открытии карты был указан неверный/утраченный номер телефона и сообщение с кодом 3D Secure приходит на неверный номер;
- сайт или страна внесены в черный список и считаются высокорискованными;
- не разрешены браузерами cookie и т. д.

Для выяснения причин Держателю карту необходимо обратиться в Банк.

7.13. Для отмены платежа, полной или частичной, Держателю карты необходимо обратиться в службу поддержки клиентов интернет-магазина для инициирования возврата платежа.

7.14. Необходимо внимательно анализировать адрес сайта (URL), на который идет переадресация. В большинстве случаев фишинга, несмотря на то что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (*например, заканчиваться на .com вместо .gov*).

7.15. Клиент может самостоятельно отключить/включить доступ к проведению интернет-платежей через мобильное приложение Банка нажав на карту, в разделе «Настройки» - Интернет-платежи и лимиты.

8. Получение наличных денежных средств в банкомате.

8.1. Перед использованием банкомата необходимо осмотреть его на наличие нехарактерных ему устройств: неровно установленной PIN-клавиатуры, накладок над экраном банкомата и иных подозрительных устройств. В случае наличия подозрительных устройств требуется воздержаться от совершения операций в таком банкомате, по возможности сообщить о своих подозрениях сотрудникам Банка по телефону, указанному на банкомате или позвонив в Контакт-центр.

8.2. Получение наличных денег в банкомате подтверждается PIN-кодом и производится Держателем карты в режиме самообслуживания, согласно инструкциям, описанных на экране банкомата.

8.3. Для того, чтобы отказаться от услуги, необходимо отменить операцию нажатием кнопки «Отмена»/«Cancel».

8.4. При наборе PIN-кода убедитесь, что его не видят посторонние. В случае если Вы введете неправильно PIN-код 6 раз, карта будет заблокирована и может быть изъята банкоматом.

8.5. Не принимайте для проведения транзакций помощь, предлагаемую третьими лицами.

8.6. За пределами Кыргызской Республики как правило в банкоматах выдача наличных осуществляется в валюте страны, при этом банки-эквайеры (владельцы банкоматов) могут устанавливать дополнительную комиссию за выдачу наличных денежных средств. Кроме того, у банка-эквайера могут быть установлены свои лимиты на сумму выдачи наличных и количество транзакций.

8.7. Сумма одной операции, снимаемой Держателем карты через свой банкомат, не должна превышать 40 000 (сорок тысяча) сом или ее эквиваленте в иностранной валюте. В банкоматах других банков одноразовая сумма снятия денежных средств может отличаться, но быть не более 20 000 (двадцать тысяч) сом или в эквиваленте этой суммы в иностранной валюте.

8.8. Одновременно с выдачей наличных денег банкомат вернет карту и распечатает квитанцию.

8.9. В случае снятия денежных средств посредством устройств необходимо поднести устройство к значку NFC на банкоматной панели. После считывая устройства банкомат потребует внести сумму и PIN-код. Выдача одной операции посредством устройств осуществляется согласно п.8.7.

8.10. Рекомендуется сохранять получаемые через банкомат квитанции, так как она заверена PIN-кодом и является подтверждением сделки.

8.11. После завершения операции снятия денежных средств посредством карты на экране банкомата появится надпись: «Заберите свою карту» и/или будут выданы наличные средства. Необходимо забрать карту (в случае снятия денежных средств с помощью физической карты) и деньги в течение 20 секунд, иначе сработает система защиты: банкомат заберёт карту и деньги обратно. Это предусмотрено в целях предотвращения забытых карт и снижения риска потери средств.

8.12. В случае изъятия банкоматом карты или денежных средств, не покидайте банкомат сразу - убедитесь, что они действительно не выданы. В некоторых случаях устройство может автоматически вернуть карту или деньги с небольшой задержкой.

8.13. Карточная операция для действующей карты при наборе правильного PIN-кода может быть отклонена по следующим причинам:

- Запрашиваемая сумма не может быть выдана банкнотами, имеющимися в кассетах банкомата. Следует запрашивать сумму, кратную минимальному номиналу банкнот, указываемому в инструкции к данному банкомату.
- Запрашиваемая сумма превышает лимит разовой выдачи, определяемый габаритами устройства выдачи наличных денег банкомата. Необходимо разделить запрашиваемую сумму на части и повторить операцию несколько раз.
- Запрашиваемая сумма превышает доступную Держателю карты сумму денег. Можно запросить меньшую сумму, размер которой можно уточнить, вызвав функцию распечатки остатка денег на карт-счете.
- Запрашиваемая сумма превышает суточный лимит доступный Держателю карты по устройству. Следует обратиться в отделение банка, где открыт счет, для снятия необходимой суммы через кассу банка.
- При обналичивании денежных средств в банкомате, убедитесь, что банкомат обслуживает карточки нужной Вам платежной системы (обычно на банкоматах располагаются логотипы платежных систем, которые обслуживаются банкоматом, согласно п.6.1.).

9. Перевод денежных средств с карты на карту.

9.1. Перевод можно осуществить через мобильный банкинг/интернет-банкинг Банка.

9.2. Перевод может быть также выполнен через сторонние мобильные приложения и платёжные сервисы, поддерживающие функцию перевода.

9.3. Для перевода денежных средств посредством данных услуг необходимо указать номер карты получателя, а в некоторых случаях — срок её действия, а также сумму перевода.

10. Пополнение карточного счета.

10.1. Пополнить карт-счет можно одним из следующих способов:

- наличными в любом филиале или сберкассе Банка;
- безналичным переводом из других банков (предварительно необходимо уточнить реквизиты карт-счёта/карты, возможен перевод по номеру телефона);
- в платежных терминалах Банка, АДМ (бесплатно);
- через другие платёжные терминалы и электронные платёжные сервисы, поддерживающие пополнение банковских карт, согласно действующим тарифам;
- безналичным переводом через мобильные приложения.

11. Случаи изъятия карты.

11.1. Причины изъятия карты банкоматом:

- занесение карты в «жёсткий» стоп-лист (заблокирована) со стороны Банка-эмитента;
- при неправильном вводе PIN-кода карты более 3 (трех) раз;
- истечение срока действия карты;
- сбой связи;
- неисправность банкомата.

11.2. В случае изъятия карты банкоматом необходимо следовать следующим действиям:

- убедиться, что карта действительно изъята и не будет возвращена автоматически;
- связаться с банком, обслуживающим банкомат — его контактные данные указаны на корпусе устройства или поблизости;
- при обращении сообщить ситуацию и уточнить порядок возврата карты;
- если банк-эквайер не установлен, следует обратиться в Банк-эмитент, указав точное местоположение банкомата (страна, город, адрес);
- при получении карты необходимо предъявить удостоверение личности.

В целях безопасности и оперативности рекомендуется при изъятии карты банкоматом, не дожидаться изъятия карты, а перевыпустить карту.

12. Что делать при утере/краже карты.

- В случае утери или кражи карты необходимо немедленно заблокировать её в мобильном приложении Банка, нажав на карту, раздел «Настройки». Либо обратиться в Банк для её блокировки, это можно сделать устно или письменно в любом филиале Банка, либо по телефону контакт-центра.
- Контакт–центр Банка: **+996 (312) 61-00-61 или 6111 (круглосуточно).**

12.1. Чем раньше Банк будет уведомлен об утере/краже карты или компрометации её реквизитов, тем ниже риск несанкционированного использования карты третьими лицами.

12.2. Держатель карты несет ответственность за все операции, совершенные до момента фактической блокировки карты. После блокировки ответственность за дальнейшие операции снимается.
Если ранее заявленная как утерянная, похищенная или скомпрометированная карта будет найдена Держателем, необходимо незамедлительно уведомить об этом Банк. Не рекомендуется пытаться воспользоваться такой картой - она может быть изъята банкоматом. Для восстановления доступа требуется обратиться в Банк для разблокировки или перевыпуска карты. В случае, если карта была разблокирована по инициативе Держателя, вся ответственность за возможные несанкционированные операции возлагается на него. Банк настоятельно рекомендует проверять выписку по карт-счёту в последующие месяцы, чтобы убедиться в отсутствии несанкционированных транзакций.

12.3. Если карта была найдена посторонним лицом, или к ней имели доступ третьи лица рекомендуется перевыпустить карту во избежание компрометации данных и несанкционированных операций.

13. Нештатные ситуации в платежной системе.

13.1. 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.).

13.2. В случае возникновении данных ситуаций в платежной системе, Банк не несет ответственности за исполнение обязательств по Договору.

13.3. Банк принимает все возможные меры для обеспечения бесперебойного функционирования оборудования и систем, участвующих в процессе предоставления услуг по карточным операциям.

14. Подозрительные операции по карте.

14.1. В случае обнаружения спорной операции в выписке по карт-счету, необходимо обратиться в отделение Банка для выяснения той или иной проведенной суммы, либо обратиться по чат-бот каналу в приложении Банка. В случае несанкционированного использования средств по карте, необходимо написать претензионное заявление. Комиссия за рассмотрение претензии удерживается согласно тарифам Банка.

14.2. В случае подозрения на совершение мошеннических/нехарактерных действий по карте, Банк вправе заблокировать карту до момента уточнения/подтверждения у Держателя карты.

14.3. Претензионное заявление на корректность операции предъявляется в течение 120 (сто двадцати) календарных дней с момента совершения операции. По истечению данного срока Банк имеет полное право не принимать претензионное заявление от Держателя карты.

14.4. По картам VISA минимальная сумма оспаривания по международным операциям составляет 15 долларов, или эквивалент в национальной валюте.

14.5. Процесс разрешения споров происходит следующим образом:
- после предоставления письменного заявления Держателя карты, Банк проводит расследование по претензионной операции на наличие соответствия действительности проведения операции. Банк имеет право запросить дополнительные документы (чек при оплате, чек при снятии денег в АТМ итд), подтверждающие факт совершения операции;
- в случае факта подтверждения некорректного списания денежных средств не по вине Держателя, Банк производит возврат денежных средств.
- срок рассмотрения претензии и принятие решений Банком в зависимости от причин может занять до трех месяцев.

14.6. Банк отказывает в удовлетворении претензий Держателя относительно недостач(и) при получении им денежных средств в банкомате в случае отсутствия излишек в банкомате, определяемых посредством ревизии/пересчета денежных средств банкомата, произведенных на основании письменного заявления Держателя.

14.7. Банк обязан своевременно сообщить информацию Уполномоченному Органу, согласно действующему законодательству КР в случае обнаружения факта наличия проведения подозрительных операций, в том числе мошеннических, по карте Держателя.

15. Правила безопасности для Держателей карт в целях предотвращения мошенничества по картам.

15.1. Запрещено передавать, продавать, дарить или иным способом предоставлять третьим лицам свою банковскую карту, включая саму карту, а также любые средства доступа к ней.
15.2. Не сообщайте посторонним лицам полный номер карты, CVV код, имя на карте, PIN-код, одноразовые пароли, отправляемые банком, 3D-secure пароль. Это конфиденциальная информация, с помощью данной информации мошенники могут получить доступ к вашим денежным средствам.
15.3. Храните карту в безопасном месте. Не оставляйте в местах, где кто-то сможет ее взять и/или скопировать номер карты/образец подписи/CVV код/имя и фамилия на карте и иные карточные данные.
15.4. Необходимо хранить в секрете PIN-код. Сообщение PIN-кода третьему лицу (родственнику, коллеге, друзьям и т.д.) может привести к несанкционированному использованию карты, то есть расходованию принадлежащих Держателю денежных средств. Операции, проведенные с вводом PIN-кода признаются совершенными Держателем карты и оспариванию не подлежат.
15.5. Запрещено хранить карту рядом с PIN-кодом (в случае его наличия), запрещено записывать PIN-код на саму карту или в документы, хранящиеся рядом с картой.
15.6. При совершении покупки нельзя терять карту из виду. Необходимо забрать карту сразу же после завершения транзакции и удостовериться в достоверности карты.
15.7. Держатель карты обязан обеспечить безопасность карты и устройства. Если иное лицо получит доступ к Вашему устройству, то это может привести к возможности совершения операции с использованием Вашей карты и/или устройства. В данном случае необходимо заморозить/заблокировать карту через мобильное приложение Банка.
15.8. В торговых точках все операции с картой должны производиться в Вашем присутствии.
15.9. До проведения операции в банкомате, обратите внимание, нет ли каких-либо внешних признаков неисправности банкомата, обнаружив рядом с ним или на нем, посторонние устройства, сообщите об этом в банк, обслуживающий данный банкомат, и воспользуйтесь другим банкоматом.
15.10. Не пользуйтесь теми банкоматами, на экране которых отражается сообщение с просьбой о переходе на другие банкоматы. Банки не помещают подобные сообщения.
15.11. По возможности, старайтесь пользоваться банкоматами, с которыми Вы уже знакомы. В других случаях, выберите банкоматы в хорошо освещенных и удобных местах расположения.
15.12. Не позволяйте никому отвлечь Вас, когда находитесь у банкомата.
15.13. Рекомендуется хранить все чеки, для последующего контроля расходов, и не выбрасывать чеки в контейнер для мусора в публичном месте.
15.14. Банк настоятельно рекомендует не вводить карточные данные (нанесенные на самой карте) при запросе сомнительных интернет сайтов, а также при запросе производителей любых мобильных телефонов (в случае неуверенности или ограниченной/отсутствия информации), поскольку в противном случае есть риск похищения или удержания денежные средства без ведома Держателя.
15.15. По возможности, рекомендуется использовать банкоматы в течение светового дня, а ночью выбирать хорошо освещенные места и убедиться в том, чтобы посторонние лица не стояли слишком близко при совершении транзакции.
15.16. При вводе PIN-кода необходимо убедиться, чтобы PIN-код не видели посторонние лица.
15.17. Для обеспечения контроля за операциями с использованием карты рекомендуется пользоваться услугой Push-уведомление или «SMS оповещение». Услуга подключается через мобильное приложение Банка.
15.18. Необходимо обновлять предоставленные в Банк контактные данные, чтобы у Банка была возможность связаться с Держателем по телефону/электронной почте/СМС, например, в случае подозрительной операции по карте.
15.19. Следуйте принципам безопасного поведения в интернете и не переходите по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты, через социальные сети, мессенджеры и т.п. или от незнакомых лиц.
15.20. Не загружайте вложенные файлы из сообщений электронной почты, которых вы не ожидали.
15.21. Обеспечьте надежной защитой свои пароли и не сообщайте их никому.
15.22. Не сообщайте никому свои персональные данные - будь то по телефону, лично или в сообщении эл. почты.
15.23. Внимательно проанализируйте адрес сайта (URL), на который Вы были переадресованы. В большинстве случаев фишинга, несмотря на то, что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (например, заканчиваться на .com вместо .gov).
15.24. Поддерживайте свой браузер обновленным и своевременно устанавливайте обновления безопасности
15.25. Банком введен запрет на проведение банковских операций, связанных с игорной деятельностью, букмекерскими конторами и казино (включая интернет пространство) и иные запрещенные виды.

16. Ограничения по Картам.

16.1. В целях снижения риска осуществления несанкционированных карточных операций Банк вправе устанавливать ограничения и лимиты на осуществление карточных операций. Величина ограничений и

лимитов, а также условия, сроки и порядок их установления, определяются Банком самостоятельно. Банк устанавливает суточные лимиты по картам. Держатель карты имеет возможность осуществлять операции с использованием Карты в пределах суточных лимитов, список которых приведен на сайте Банка www.bakai.kg.

16.2. Банк может приостановить, ограничить или удалить токенизированную карту с устройства, если это необходимо по причинам безопасности, закрытия или перевыпуска карты, соблюдения требований законодательства Кыргызской Республики.

16.3. Стандартные ограничения, установленные Банком, могут быть изменены Клиентом через мобильное приложение самостоятельно или по письменному обращению Держателя в Банк в рамках разрешенных лимитов.

16.4. Банком установлены дополнительные ограничения по бесконтактным картам:
- проведение транзакций без ввода PIN-кода в пределах установленных лимитов согласно тарифам Банка;
- проведение транзакций с вводом PIN-кода свыше установленных лимитов согласно тарифам Банка.

17. Срок действия карты и расторжение Договора.

17.1. На карте указывается дата истечения срока ее действия (месяц и год). Карта действительна до конца последнего дня, указанного на ней месяца. Все просроченные карты блокируются и подлежат сдаче в Банк.

17.2. Держатель вправе закрыть карту и расторгнуть Договор в одностороннем порядке путем предоставления заявления на аннулирование карты.

17.3. Банк вправе блокировать/аннулировать карту и расторгнуть Договор с Держателем при невыполнении Держателем условий настоящих Правил и Договора.

17.4. При расторжении Договора Держатель должен погасить имеющуюся перед Банком задолженность и сдать все карты, оформленные по его карт-счету.

17.5. В случае расторжения Договора по инициативе любой из сторон комиссия за годовое обслуживание и иные уплаченные Держателем комиссии не возвращается.

17.6. Остаток денежных средств по карт-счету выдается при отсутствии задолженности перед Банком.

18. Процесс подключения карты к Digital Wallet.

18.1. Для подключения карты к Digital Wallet необходимо:
- наличие устройства (смартфон/Apple Watch/Garmin/ iPad/Mac) на базе Apple (версии 6 и новее) и Android (версии 4.4 и выше) поддержкой технологии NFC;
- установленное мобильное приложение Банка;
- активированный экран блокировки с установленным паролем, PIN-кодом или биометрической защитой.

18.2. Подключение карты через мобильное приложение Банка осуществляется следующим образом:
- открыть мобильное приложение Банка и выбрать нужную карту;
- нажать на значок «Pay»;
- следовать инструкциям на экране, включая ввод личной информации и подтверждение согласия с условиями использования.

18.3. После успешного подключения на изображении карты в мобильном приложении отобразится иконка Apple Pay/Google Pay, подтверждающая готовность к использованию.

18.4. Для оплаты в торговых точках необходимо:
- включить NFC на устройстве;
- разблокировать устройство;
- поднести устройство к POS-терминалу.

19. В отдельных случаях (например, при оплате крупных сумм или подряд нескольких покупок) устройство может запросить пароль разблокировки смартфона. Ввод PIN-кода карты не требуется.

20. Прочие условия.

20.1. В течение 5 (Пяти) дней извещайте Банк обо всех изменениях в данных, указанных в Заявлении-анкете и иных документах, связанных с выпуском карты путем предоставления Банку документов, содержащих изменения. За последствия несвоевременного извещения об изменении этих данных Банк ответственности не несет.