Меры безопасности при использовании банковских карт

1. Общие меры безопасности и минимизация рисков

1.1. При получении Карты обязательно проставьте на ней свою подпись.

1.2.ПИН-код (персональный идентификационный номер) – это комбинация цифр, содержащая 4 знака и предназначенная для идентификации Держателя Карты, а также для защиты от несанкционированного использования Карты. **Информация о ПИН–коде должна быть известна только Вам. Никто не вправе просить Вас сообщать ПИН–код Карты.**

1.3. Не храните ПИН-код и Карту вместе, не записывайте ПИН–код на самой Карте. Запомните ПИН–код, либо храните его отдельно от Карты в недоступном для других лиц месте.

1.4. Не передавайте Карту посторонним лицам для проведения каких-либо операций.

1.5. Для снижения риска проведения мошеннических операций при посещении стран с высоким уровнем мошенничества (страны Африки, страны Юго-Восточной Азии, страны Латинской Америки, Молдавия, Украина, Турция, США) особенно тщательно соблюдайте все меры безопасности, изложенные в данной Памятке.

1.6. Сохраняйте чеки, подтверждающие оплату товаров и услуг, в течение года со дня совершения операции по Карте. Если сделка, по каким-либо причинам не состоялась, сохраняйте чеки о неуспешных операциях с использованием Карты и/или альтернативной оплате (оплата наличными, с использованием другой Карты), в случае ее проведения. Указанные документы могут потребоваться для подтверждения правомерности операции, совершенной с использованием Карты, или для урегулирования спорных ситуаций.

1.7. **Регулярно (не реже одного раза в месяц) проверяйте выписки по банковскому счету. При возникновении вопросов, связанных с проведенными операциями по счету (несанкционированными списаниями или ошибочными начислениями), незамедлительно обратитесь в отделение ЗАО «КИКБ» (далее Банк).**

1.8. Для контроля за состоянием банковского счета и перечнем операций Вы можете воспользоваться услугой i-bank - система дистанционного банковского обслуживания ЗАО «КИКБ» и/или выпиской, которую можете получить в Банке.

1.9. Для обеспечения контроля за операциями с использованием Карты Вы можете воспользоваться услугой «SMS оповещение». С помощью данной услуги Вы можете получать информацию о доступном остатке после совершения операций по Карте, уведомления о поступлении денежных средств на счет и расходных операциях по счету.

Услуги, указанные в пп. 1.8. и 1.9., подключаются на основании заявления от картодержателя.

1.10. Для минимизации финансовых потерь от проведения мошеннических операций по Вашей Карте, Вы имеете возможность установить ограничения по суммам операций с Картой (по каждой операции, по операциям в течение 24 часов), как отдельно для операций безналичной оплаты товаров (работ, услуг) и/или операций получения наличных денежных средств, так и для всех операций. С этой же целью Банком может быть установлено ограничение на получение наличных денежных средств на банкоматах в течение суток.

1.11. При получении любых запросов (по электронной почте, телефону и иным способом) с просьбой подтверждения персональных данных и сведений о Вашей Карте не передавайте информацию по Вашей Карте **(ПИН-код, номер Карты, срок окончания действия Карты, CVV2 – код безопасности)**, так как данные сообщения используются злоумышленниками в целях получения конфиденциальной информации для последующего использования в мошеннических целях. Будьте внимательны: сообщения могут быть похожи на настоящие официальные сообщения (могут иметь стиль делового письма, содержать ссылки на действующие сайты или сайты, хорошо замаскированные под сайты известных организаций, информирование может осуществляться в автоматическом режиме с использованием «электронного голоса»), а также могут передавать вредоносные программы, являющиеся компьютерными вирусами, позволяющие неправомерно получать персональную информацию. При получении подобных сообщений (запросов) незамедлительно свяжитесь по телефону с «Колл центром» Банка. Для информационного взаимодействия с Банком используйте средства связи (телефоны/факсы, интернет-банкинг. обычная и электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.

1.12. Для безопасного использования Интернет-ресурсов пользуйтесь адресами официальных Web-сайтов Данные меры связаны с появлением в сети Интернет Web-сайтов, имитирующих интернет-представителей Банков Кыргызской Республики. Доменные имена (адреса, по которым компания предлагает услуги через сеть Интернет) и стиль оформления данных сайтов, как правило, сходны с именами подлинных Web-сайтов банков. Использование подобных реквизитов сопряжено с риском и может привести к нежелательным последствиям (в том числе к финансовым потерям). В случае самостоятельного выявления ложного Web-сайта Банка или получения сведений подобного рода по электронной почте или иным способом, незамедлительно свяжитесь по телефону (312) 97 67 97 или 62 01 01 с Колл центром Банка.

2. Меры предосторожности при совершении операций с использованием Карты

Скимминг (от англ. skimming) — кража данных карты при помощи специального считывающего устройства (**скиммера**). Злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и **CVC-код**), **ПИН-код** воруют с помощью мини-камеры или накладок на клавиатуру, установленных на **банкоматах**.

2.1. Совершайте все операции с Картой в торгово-сервисных предприятиях только в Вашем присутствии. Не разрешайте сотрудникам торгово-сервисной предприятий уносить Вашу Карту в другое помещение и не допускайте потери Карты из поля Вашего зрения при проведении операций, так как в подобных случаях информация с Вашей Карты при помощи специальной аппаратуры (скиммер) может быть скопирована и использована для изготовления поддельной карты с целью получения доступа к Вашему банковскому счету.

2.2. Перед тем как поставить подпись на чеке, убедитесь в том, что в документе правильно указаны все данные о совершаемой операции. Если Вы обнаружили неточности в указанной информации, откажитесь от проставления подписи и попросите сделать отмену проведенной операции. В случае отмены операции необходимо получить чек об отмене операции.

2.3. Не оставляйте в торгово-сервисных предприятиях незаполненные чеки с оттиском Вашей Карты т.е. чеки, на которых отсутствует Ваша подпись или сумма операции. Незаполненные, а также «**испорченные»** чеки должны уничтожаться сотрудником торгово-сервисной организации сразу же в Вашем присутствии.

2.4. Не выбрасывайте и не оставляйте в торгово-сервисных организациях платежные документы по операциям с Картой, так как на них может быть отпечатан полный номер Карты.

2.5. При вводе ПИН-кода во время совершения операции в торгово-сервисном предприятии обратите внимание на то, чтобы он вводился на специальном устройстве (ПИН-паде или посредством самого ПОС-терминала), непосредственно соединенном с кассовым аппаратом или ПОС-терминала. Не поддавайтесь на предложение ввести ПИН-код дважды на различных устройствах в одном и том же месте, за исключением случаев повторной оплаты или отмены операции.

2.6. Обращаем Ваше внимание на то, что сотрудник банка или торгово-сервисного предприятия при проведении операции по Карте вправе потребовать документ, удостоверяющий Вашу личность.

2.7. Карта может быть изъята у Вас по требованию Банка сотрудником банка или торгово-сервисных предприятий, в которых Вы осуществляете оплату товаров/услуг с помощью Карты. В этом случае Вам необходимо обязательно получить акт об изъятии Карты и незамедлительно связаться с Банком для произведения блокирования карты.

2.8. Не забудьте забрать Карту после совершения операции, убедившись при этом, что возвращенная Карта принадлежит Вам.

2.9. Предъявляйте Карту к оплате только в тех торгово-сервисных предприятиях, которые вызывают доверие. Соблюдайте особую осторожность при проведении операций с использованием Карты в следующих торгово-сервисных организациях:

- развлекательные центры
- ювелирные салоны
- туристические агентства

- интернет-услуги (заказ билетов, оплата товаров/услуг, бронирование отелей и т.д.)

Особенно важно помнить об этом во время путешествий в странах Восточной Европы, Азиатско-Тихоокеанского региона, в странах с высоким уровнем мошенничества, указанных в п. 1.5.

2.10. Для минимизации рисков Вашей Карты воздержитесь от получения наличных денежных средств в торгово-сервисных предприятиях, которые помимо продажи товаров занимаются обналичиваем денежных средств. Используйте для этих целей пункты выдачи наличных или банкоматы, находящиеся в безопасных местах (подразделения банка, государственные учреждения, крупные торговые комплексы, гостиницы, аэропорты и т.п.).


2.11. Перед проведением операции на банкомате/терминале самообслуживания осмотрите его внешний вид. При обнаружении устройств, вызывающих подозрение (накладка на устройстве для чтения карты, накладка на клавиатуре для ввода PIN-кода, накладка на лицевой стороне банкомата или рядом с ним, в которую может быть вмонтирована камера и т.п.), проводов и посторонних изделий не вставляйте Карту в устройство для чтения. По возможности свяжитесь с организацией, установившей банкомат/терминал самообслуживания для уведомления об обнаруженных подозрительных устройствах.

2.12. В целях предотвращения мошеннических операций и согласно рекомендациям международных платежных систем Банком устанавливаются на банкоматы специальные типовые накладки, позволяющие избежать несанкционированного копирования данных магнитных дорожек карт. В случае наличия информации на экране банкомата о внешнем виде антискимминговой накладки для дополнительного обеспечения безопасности сверьте внешний вид имеющейся накладки с предлагаемым изображением. При выявлении несоответствия свяжитесь по телефону с Колл центром.

2.13. Если поблизости с банкоматом Вами замечены подозрительные люди, рекомендуется выполнить операцию на другом банкомате, установленном в хорошо освещенном и безопасном месте, либо в пункте выдачи наличных денежных средств.

2.14. Обращаем Ваше внимание на следующее: считыватель банковских карт для обеспечения доступа в специальные закрытые помещения, где устанавливаются банкоматы и другие терминалы самообслуживания, не должен требовать ввода ПИН–кода. Если при входе в помещение установлено устройство, требующее ввод ПИН–кода, не пользуйтесь им.

2.15. При проведении операции с вводом ПИН–кода проследите, чтобы вводимый на клавиатуре ПИН-код не был виден окружающим, для этого, например, другой рукой закройте клавиатуру для избежания возможности видеозаписи Ваших действий и просмотра информации о вводимом ПИН-коде со стороны. Не прибегайте к помощи посторонних лиц при проведении операций по Картам.

2.16. В случае захвата Вашей Карты банкоматом/устройством самообслуживания вследствие возникновения технических проблем, незамедлительно свяжитесь с Банком, обслуживающей банкомат/устройство самообслуживания для уточнения информации, когда и где будет можно получить Карту. Рекомендуется временно приостановить действие Карты (временно заблокировать Карту), связавшись по телефону в Колл центр Банка.

2.17. В случае неполучения всей либо части запрошенной суммы на банкомате или возникновения проблем при совершении операции вложения (на устройствах с функцией приема наличных денежных средств) обратитесь в Банк для оформления заявления о возникшей проблеме.

- **В случаях, когда Вам кажется, что Ваш ПИН–код стал известен посторонним людям, у Вас возникли подозрения в незаконном использовании Вашей Карты, Карта была утеряна, украдена или захвачена банкоматом, Вам следует незамедлительно связаться по телефону с Колл Центром Банка, либо лично обратиться в Банк с просьбой заблокировать Карту и заказать новую Карту.**

3. Меры безопасности при совершении операций безналичной оплаты товаров (работ, услуг) посредством сети Интернет, телефона/факса, почты.

3.1. При проведении операций безналичной оплаты товаров/услуг посредством сети Интернет, телефона/факса, почты Вас могут попросить указать CVV2 (три цифры кода безопасности). Данное значение находится на оборотной стороне Карты (три последних цифры, напечатанные на полосе для подписи или справа от нее в специальном поле) и служит для дополнительной проверки клиента Банком.

3.2. Ввод ПИН-кода для идентификации Держателя предполагается только при проведении операций с Картой в присутствии самого Держателя на терминалах с функцией чтения данных карты и только при помощи специального устройства – ПИН-пада: клавиатуры, соединенной с платежным терминалом либо кассовым аппаратом. В случае проведения операций безналичной оплаты товаров/услуг посредством сети Интернет, телефона/факса, почты следует исключить предоставление информации о ПИН-коде.

3.3. При проведении операций в Интернет-магазинах проконтролируйте, что магазин имеет опубликованные обязательства по защите данных клиента, сертифицирован платежной системой VISA и на сайте присутствует контактные данные организации. По возможности убедитесь в правильности адреса и телефона, указанных на сайте. Ввод необходимых данных должен проходить в защищённом канале с использованием HTTPS-протокола.

3.4. Будьте внимательны, Web-сайты могут использоваться мошенниками в целях получения конфиденциальной информации (для заказа товара/услуги клиентам предлагается заполнить электронные формы и указать реквизиты банковских счетов, карт, включая ПИН-код). Встречаются, например, такие виды мошенничества как **сайт-близнец** известного Интернет-магазина; «магазин-однодневка»; сайт, который представляет реально не существующую организацию и пр. **С осторожностью относитесь к проведению операций посредством сети Интернет и предоставлению Вашей персональной информации и информации о Ваших Картах.**

3.4**.** В целях избежание мошенничества по Вашей Банковской карте, Банк советует Вам после использования Банковской карты в одной из нижеуказанных стран обратиться в ЗАО "КИКБ" за блокированием или перевыпуском Вашей карты на новую карту:

• Таиланд	• Мексика	• Вьетнам
• Малайзия	• Нигерия	• Индия
• Тайвань	• Украина	• Китай
• Бразилия	• Турция	• Австралия
• Гонконг	• США	• ОАЭ
• Индонезия	• Россия	• Сингапур
• Болгария	• Испания	• Молдавия

Следует помнить:

- **Банк не несет ответственность за операции, возникшие в результате скимминга (подделки) карты.**
- **Банк не несет ответственность за транзакции, совершенные на мошеннических сайтах.**
- **Клиент несет ответственность за все операции, совершаемые по Карте (включая Интернет-операции), совершенные с использованием реквизитов карточки, а также за все суммы, списанные со счета клиента.**
- **Клиент несет все риски, связанные с проведением Интернет-операций.**
- **Банк не несет ответственность в случае, если операция не проходит по независящим от Банка обстоятельствам.**