

Уважаемые клиенты - держатели банковских платежных карт ОАО «Бакай Банк»

С целью повышения уровня безопасности Ваших карт мы предлагаем Вам ознакомиться с нашими рекомендациями. Это позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН-кода и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты.

Наши рекомендации:

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.

Не записывайте ПИН-код на самой карте. Не храните вместе ПИН-код и карту. Запомните ПИН-код, либо храните его отдельно от карты в недоступном для других лиц месте.

При получении карты обязательно проставьте на ней свою подпись.

Не передавайте карту посторонним лицам для проведения каких-либо операций.

В случае **утери** или **кражи** карты Вашей платежной карты немедленно свяжитесь с Банком или с ЗАО Межбанковский Процессинговый Центр», контактный номер которого находится на обратной стороне карты.

Не реже одного раза в месяц проверяйте выписки карточного счета. При возникновении вопросов, связанных с проведенными операциями по счету (несанкционированными списаниями или ошибочными начислениями), незамедлительно обратитесь в отделение ОАО «Бакай Банк» (далее Банк).

Для контроля, за состоянием карточного счета и перечнем операций Вы можете воспользоваться услугой «**Интернет Банкинг**» - система дистанционного банковского обслуживания ОАО «Бакай Банк» или выпиской, которую можете получить в Банке.

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. **Внимание! При поступлении SMS-сообщения по операции, которую Вы не совершали, необходимо срочно заблокировать карту**

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 (номер Карты, срок окончания действия Карты, CVV2 – код безопасности, ПИН-код), 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.

Для безопасного использования Интернет-ресурсов пользуйтесь адресами официальных Web-сайтов. 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 **0 (321) 61 00 61** с Колл центром Банка или отправьте сообщение по электронному адресу fraud@bakai.kg

Нужно знать:

- ✓ **Банк не несет ответственность за транзакции, совершенные на мошеннических сайтах.**
- ✓ **Банк не несет ответственность в случае, если операция не проходит по независящим от Банка обстоятельствам.**
- ✓ **Клиент несет все риски, связанные с проведением Интернет - операций.**
- ✓ **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.**
- ✓ **Банк не несет ответственность за скимминговые операции.**

В целях избежание мошенничества по Вашей платежной банковской карте, Банк советует после использования платежной банковской карты в одной из нижеуказанных стран обратиться в ОАО "Бакай Банк" за перевыпуском на новую карту или блокированием Вашей карты.

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