ПАМЯТКА
ДЕРЖАТЕЛЯ БАНКОВСКИХ КАРТ КБ «МКБ» (ПАО)

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

1.Общие рекомендации

1.1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты. **ПИН-код должен быть известен только Вам.** Ввод ПИН-кода производится для подтверждения операций, проводимых в банкоматах и электронных терминалах. При проведении операции с вводом ПИН-кода прикрывайте клавиатуру свободной рукой. Это не позволит мошенникам подсмотреть Ваш ПИН-код или записать его на видеокамеру.

1.2. **Запрещается хранение данных о ПИН-коде на любых носителях.**

1.3. Право использовать банковскую карту имеет только то физическое лицо, чьи фамилия и имя нанесены на карту.

Не разглашайте реквизиты банковской карты (номер, срок действия и иные сведения), а также свои персональные данные третьим лицам.

Не передавайте карту третьим лицам, за исключением случаев передачи карты сотрудникам торгово-сервисных предприятий (далее – ТСП) и в пунктах выдачи наличных (далее - ПВН) при осуществлении Вами операций, в т.ч. оплаты товаров и услуг с помощью карты.

1.4. При получении банковской карты **активируйте ее путем введения ПИН-кода в банкоматах КБ «МКБ» (ПАО), ПАО Банка «ЗЕНИТ», банкоматах** иных кредитных организаций, и распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.

1.5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Храните свою карту в недоступном для окружающих месте, а также отдельно от наличных денег и документов, рядом с мобильными телефонами, ключами, бытовой и офисной техникой. Не сгибайте и не царапайте карту.

Если в результате повреждения карты, ее использование стало невозможным при проведении операций, незамедлительно обратитесь в Банк для ее сдачи и получения новой карты.

1.6. В целях информационного взаимодействия с Банком рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке.

Также необходимо всегда иметь при себе контактные телефоны Банка спонсора ПАО Банк «ЗЕНИТ»: **+7 (495) 937-07-35; +7 (495) 777-57-05; 8-800-500-66-77 (звонок по России бесплатный) КРУГЛОСУТОЧНО** и банка-эмитента банковской карты - КБ «МКБ» (ПАО) - **+7 (495) 748-53-53** (в рабочее время с понедельника по четверг с 9-00 до 18-00, в пятницу с 9-00 до 17-00).

Служба поддержки ПАО Банка Зенит и КБ «МКБ» (ПАО):

принимает сообщения об утрате/краже карты/подозрении в неправомерном/мошенническом использовании банковской карты и консультирует о порядке действий в этих ситуациях;

дает рекомендации о порядке действий в случае выявления спорных ситуаций или неправомерных отказов в совершении операций с использованием банковской карты,

1.7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить услугу SMS-инфо для оперативного получения уведомления о совершении операции с использованием банковской карты.

1.8. При получении электронного письма и SMS-сообщения, в которых от имени Банка предлагается предоставить персональные данные, или информацию о банковской карте (в том числе ПИН-код) не сообщайте их. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт Банка) и SMS-сообщениях, так как они могут вести на сайты-двойники и

вирусоопасные сайты (сайты с повышенной опасностью заражения вирусами). Незамедлительно при возникновении нестандартной ситуации сообщите в Службу поддержки, по телефонам указанным в п.1.6. о данном факте.

ВНИМАНИЕ!!! SMS-сообщения КБ «МКБ» (ПАО) всегда поступают с номера "mcombank", при любом информировании Клиентов указываются телефоны Банка, опубликованные на официальном сайте.

1.9. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а так же если банковская карта была утрачена, необходимо немедленно обратиться в Службу поддержки, по телефонам, указанным в п.1.6. и следовать указаниям сотрудника Службы поддержки. До момента обращения в Службу поддержки, Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета.

Для самостоятельной блокировки карты, при условии подключенной услуги SMS-инфо (с сотового телефона, номер которого был указан в Заявлении на подключение), Вам необходимо отправить сообщение **номер + 7(916) 552-4886 со следующим содержанием:**

Block /пробел/ NNNN, где NNNN- последние 4 цифры номера карты и карта незамедлительно будет заблокирована путем предоставления ответного SMS-сообщения: Карта NNNN блокирована.

Для получения в виде SMS-сообщения информации о Доступном остатке на СКС, Держателю необходимо отправить SMS-запрос с сотового телефона, номер которого был указан в Заявлении на подключение к Услуге, на номер **+7 (916) 552-4886.**

SMS-запрос должен быть составлен следующим образом:

- Balance/пробел/NNNN (последние четыре цифры номера Карты, номер которой был указан в Заявлении на подключение к Услуге).

2. Совершение операций с картой в банкомате

2.1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2.2. Если дверь в помещение, где расположен банкомат оборудована электронным замком, открываемым картой, помните, что он должен открываться без введения ПИН-кода. Если Вам предлагают ввести ПИН-код, то перед Вами устройство, установленное мошенниками.

2.3. Прежде чем провести по карте операцию через банкомат убедитесь в наличии на банкомате логотипа платежной системы, соответствующей Вашей карте, а также информации о банке, обслуживающем банкомат (название, адрес, телефон).

2.4. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с картой в банкоматах.

2.5. Не допускайте ошибок при вводе ПИН-кода. В случае если ПИН-код три раза подряд будет набран неверно, карта заблокируется на совершение операций с вводом ПИН-кода. В этом случае Вам необходимо обратиться в подразделение Банка для изменения ПИН-кода.

2.6. По завершении операции не забудьте забрать выданные деньги, карту и квитанцию банкомата (они могут возвращаться в любой последовательности). В случае если после проведения операции карта не была удалена из картоприемника по истечении 20-40 секунд, она будет задержана банкоматом.

2.7. Если банкомат задержал Вашу карту, Вам необходимо:

переписать указанные на банкомате реквизиты (название, адрес и телефон) банка, которому принадлежит банкомат;

обратиться в Службу поддержки по телефонам, указанным в пункте 1.6. и действовать в соответствии с инструкциями оператора Службы поддержки.

2.8. При приеме и возврате карты банкоматом не толкайте и не выдергивайте карту до окончания ее движения в картоприемнике.

2.9. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться

возврата карты.
2.10. В случае если клавиатура или место для приема банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
2.11. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

3. Рекомендации при использовании карты для оплаты товаров и услуг в торгово-сервисных предприятиях

3.1. Не используйте карты в организациях торговли и услуг, не вызывающих доверия.
3.2. Во избежание мошенничества с Вашей картой, а также в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте, требуйте проведения операций с ней только в Вашем присутствии, не позволяйте уносить ее из поля Вашего зрения. 3.3. Кассир Торгово-сервисного предприятия (далее – ТСП) может потребовать предъявления документа, удостоверяющего Вашу личность. В случае отсутствия документа, Вам может быть отказано в проведении операции по карте.
3.4. При осуществлении операции в ТСП с использованием электронного терминала, кассир может предложить Вам ввести ПИН-код на выносной клавиатуре электронного терминала или на клавиатуре самого терминала. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. При отказе ввести ПИН-код или неверном вводе ПИН-кода в проведении операции может быть отказано.
3.5. По завершении операции кассир должен выдать Вам документ, подтверждающий проведение операции с использованием карты (далее – квитанция) и попросить ее подписать. Несогласие подписать квитанцию также может привести к отказу в проведении операции. Перед тем как подписать квитанцию в обязательном порядке проверьте указанную в ней сумму.
Не подписывайте квитанцию, в которой не проставлены (не соответствуют действительности): вид операции, сумма операции, валюта операции, дата совершения операции, сумма комиссии (если имеет место), код авторизации, реквизиты карты, наименование ТСП.
3.6. В случае Вашего отказа от покупки сразу же после завершения операции требуйте отмены операции и убедитесь в том, что кассир ТСП уничтожил ранее оформленную квитанцию.
3.7. При возврате покупки или отказе от услуг, ранее полученных в ТСП по Вашей карте, должна быть проведена кредитовая операция – операция «возврат покупки» с обязательным оформлением квитанции, на которой должно быть указано «возврат покупки», подписанной кассиром ТСП. Непременно сохраните квитанцию на «возврат покупки» для последующей проверки на отсутствие указанной операции в выписке по Счету.
Если сумма операции не поступит на Ваш Счет в течение 15 календарных дней, обратитесь в подразделение Банка для оформления претензии.
3.8. В случае любого неправомерного, с Вашей точки зрения, отказа в проведении операции по карте рекомендуем Вам незамедлительно связаться со Службой поддержки по телефонам, указанным в п.1.6.

4. Изъятие карты

4.1. Ваша карта может быть изъята в банкомате, ПВН, а также в ТСП в случае: использования **карты, ранее заявленной как утраченная;**
использования карты с истекшим сроком действия;
использования карты третьими лицами;
использования карты после получения Вами уведомления Банка с требованием о возврате карты;
иных случаях неправомерного использования карты, включая покупку товаров и услуг, запрещенных действующим законодательством Российской Федерации.
4.2. В случае изъятия карты в ТСП или ПВН Банка требуйте расписку об изъятии с указанием даты, времени и причины изъятия, убедитесь, что изъятая у Вас карта разрезана в Вашем присутствии. Сообщите об изъятии карты в Службу поддержки по телефонам, указанным ому в пункте 1.6.

5. Совершение операций с банковской картой через сеть Интернет

5.1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
5.2. Не сообщайте персональные данные или информацию о банковской (ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций.
5.3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать **отдельную банковскую карту с предельным лимитом, предназначенную только для указанной цели.**
5.4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
5.5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий.
5.6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или) информации о банковской карте/Счете.
В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
5.7. Не передавайте полные реквизиты банковской карты (а также полный номер карты) через открытые электронные каналы информационного обмена – такие, как электронная почта, SMS-сообщения, ICQ и т.п.
Ввод полных реквизитов банковской карты допустим только в специальную платежную форму на сайте интернет - магазина при совершении покупки.
5.8. Избегайте отображения и ввода полного номера Вашей банковской карты в публичных местах – в Интернет-кафе, Интернет - терминалах и прочих общедоступных точках доступа.
5.9. Установите на свой компьютер персональные межсетевые экраны, антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ). Используйте программное обеспечение анализа безопасности Вашего компьютера и сайтов, которые Вы собираетесь посетить (свободно распространяемые программы от McAfee - Security Scan Plus, Site Advisor и др. программные продукты). Это может защитить Вас от проникновения вредоносного программного обеспечения.

6. Реквизиты Банка

«Международный коммерческий банк» (публичное акционерное общество)
Краткое наименование: КБ «МКБ» (ПАО)
Полное наименование на английском языке: «International commercial bank»
Краткое наименование на английском языке: «ICB»
Регистрационный номер лицензии ЦБ РФ: № 2524
Дата регистрации в ЦБ РФ: 05.10.1993 г.
ОГРН: 1027700053776 (23.07.2002г.)
ИНН 2465029704 КПП 775001001
БИК 044585319, Корреспондентский счет 30101810200000000319 в Отделении 2 Москва
Адрес: 115280, Российская Федерация, город Москва, Пересветов переулок, дом 2/3, подъезды №1,2.
Контактная информация:
Телефон/Факс многоканальный: +7 (495) 748 53 53
Адрес в сети Internet (веб-сайт): www.mcombank.ru, Электронная почта (E-mail):info@mcombank.ru