Ваша финансовая безопасность

Уважаемые клиенты!

ИНГ БАНК (ЕВРАЗИЯ) АО (далее – «Банк») считает обеспечение информационной безопасности одной из главных задач при работе со своими клиентами. Технологии хранения и обработки персональной информации клиентов, используемые Банком, соответствуют требованиям российских регуляторных органов и международных платёжных систем. Для обеспечения минимизации возможного ущерба от мошенничества, банковские карты выпускаются с предустановленными ограничениями (лимитами) на операции покупки и снятия наличных (которыми Вы можете управлять, позвонив по телефонам Горячей Линии Банка). Телефоны Горячей Линии Банка указаны на оборотной стороне банковской карты: +7(495) 933-47-47, +7(495) 229-73-37.

Тем не менее, обращаем Ваше внимание на то, что безопасность использования банковских карт во многом зависит от осведомлённости владельца пластиковой карты о возможных угрозах и его ответственного отношения к соблюдению правил пользования картой. Пожалуйста, внимательно прочитайте материалы раздела перед использованием Вашей карты. Напоминаем Вам, что сохранность Ваших средств зависит, в том числе и в немалой степени, от Вашего ответственного отношения к вопросам обеспечения защиты Ваших персональных данных при использовании банковской карты.

1. Общие рекомендации по мерам безопасности.

Банк выпускает пластиковые карты, которые являются инструментом доступа к денежным средствам, находящимся на Ваших банковских счетах, поэтому отношение к их использованию и хранению должно быть аналогично отношению к наличным денежным средствам. Чтобы использование банковских карт было удобным и безопасным (в ряде стран существуют ограничения на использование карт, выпущенных в РФ), а Ваши денежные средства оставались в сохранности, просим Вас обратить внимание на следующие простые правила и рекомендации:

1.1. Храните карту вне доступа третьих лиц, не передавайте карту и/или не сообщайте информацию о своей банковской карте (номер – 16 цифр на лицевой стороне карты, срок её действия, код безопасности – 3 цифры, указанные на полосе для подписи на оборотной стороне карты) третьим лицам, в том числе родственникам. Относитесь к хранению банковской карты так же, как Вы относитесь к хранению наличных денежных средств. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту;

1.2. Всегда имейте при себе контактные телефоны круглосуточной службы поддержки Держателей банковских карт Банка (Горячей Линии Банка). Перепишите номер карты и телефон Горячей Линии Банка - эта информация может пригодиться Вам в случае потери или кражи карты. Храните эту информацию в надежном месте;

1.3. Проявляйте аккуратность при хранении и вводе ПИН-кода (не храните его вместе с банковской картой). ПИН-код необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты либо ее номера, в неявном виде и недоступном для третьих лиц, в том числе родственников, месте. Исключите полностью возможность одномоментной утери карты и ПИН-кода;

1.4. В случае замены ПИН-кода на новый, придуманный Вами, избегайте очевидных, легко предполагаемых цифровых комбинаций, например: окончание Вашего номера телефона, дата Вашего дня рождения и прочее;

1.5. Никогда никому не раскрывайте свой ПИН-код. Помните, что Вы никому не должны и не обязаны сообщать его: ни родственникам, ни представителям Банка, ни представителям правоохранительных органов, ни кассирам торговых точек и лицам, помогающим Вам в использовании банковской карты. ПИН-код должен быть известен только Держателю карты;

1.6. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи Держателя банковской карты;

1.7. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте сколов, царапин и попадания на нее влаги. Банковскую карту нежелательно хранить рядом с мобильным телефоном, бытовой и офисной техникой;

1.8. Будьте бдительны при получении электронных писем или SMS-сообщений, в том числе направленных от имени Банка (например: о блокировке карты или каких-либо платежах), особенно если они содержат ссылки или номера телефонов для связи, отличные от телефонов на оборотной стороне Вашей карты. Не следуйте по ссылкам, указанным в письмах и сообщениях (включая ссылки на сайт Банка), т.к. они могут вести на мошеннические сайты;

1.9. Не перезванивайте по телефонам, которые указаны в SMS-сообщениях, вне зависимости от их содержания. Обращайтесь в Банк только по телефону Горячей Линии Банка либо по реквизитам средств связи (мобильных и стационарных телефонов, факсов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке;

1.10. Не сообщайте никакой информации о себе и Ваших картах позвонившим лицам. При возникновении подозрений звоните в Банк по телефонам Горячей Линии Банка, которые указаны на оборотной стороне банковской карты;

1.11. Никогда не сообщайте никому пароли, приходящие в сообщениях от Банка;

1.12. При звонке сотрудника Банка никогда не сообщайте ему полный номер карты или другие ее реквизиты (CVV2-код, срок действия), ПИН-код или одноразовый пароль, не устанавливайте никаких приложений по его просьбе. Если разговор с позвонившим Вам сотрудником Банка вызывает у вас сомнения, немедленно закончите этот разговор и перезвоните по телефону Горячей Линии Банка и сообщите о произошедшем;

1.13. Сотрудники Банка не могут Вам позвонить вне пределов рабочего времени Банка – рано утром, поздно вечером, ночью, а также в выходной или в праздничный день;

1.14. Сотрудники Банка никогда не совершают звонков для выяснения реквизитов карты, вне зависимости от определившегося номера телефона;

1.15. Помните, что в случае раскрытия ПИН-кода, 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-кода, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в Банк и следовать указаниям сотрудника Банка;

1.16. Никогда не передавайте номер своей карты, а также других ее реквизитов, по телефону каким-либо лицам или компаниям, если Вы не уверены в том, что запрашивали какие-то услуги предварительно (например: аренда машин, гостиниц);

1.17. Не устанавливайте никакие приложения по ссылкам, приходящим на Ваш телефон по любым каналам связи (SMS, электронная почта, мессенджеры и т.д.);

1.18. Никогда не принимайте советов и не используйте помощь третьих лиц при проведении операций с картой;

1.19. Используйте услугу «SMS-Банкинг» (услуга платная, размер платы уточняйте в разделе «Услуги для сотрудников корпоративных клиентов») или ее бесплатный аналог с базовым функционалом - сервис «SMS-информирование» для контроля операций по своим банковским картам. Оперативное получение SMS-уведомлений по операциям с Вашей банковской картой и возможность моментальной самостоятельной блокировки банковской карты (доступно только пользователям услуги «SMS-Банкинг»), без телефонного звонка в Банк, позволит Вам своевременно отреагировать на несанкционированный доступ к карточному счету;

1.20. Переводите на счет карты с текущего счета только необходимую сумму для ближайших запланированных операций. Это может помочь Вам в том числе в случае потери карты вместе с ПИН-кодом обойтись без существенных потерь денежных средств;

1.21. Не реже раза в месяц получайте выписку по Вашим счетам в отделении Банка или оформите Заявление о ежемесячном предоставлении ее Вам по электронной почте (комиссия за данную услугу не взимается). Из-за специфики проведения расчетов через платежные системы, только из выписки можно узнать полную информацию об операциях по счету. Эта информация позволит Вам своевременно заявить в Банк о несогласии с операцией (например: в случае повторного списания средств по ранее уже оплаченной Вами операции). Воспринимайте SMS-уведомления об операциях только как дополнительный источник информации;

1.22. Всегда проверяйте свою выписку по счету, особенно после возвращения из поездки. Сверьте суммы покупок, оплаченных по карте, с имеющимися у Вас чеками. Проверьте выписку: не указаны ли в ней неизвестные транзакции, сделанные не Вами;

1.23. Не отключайте без необходимости Ваш мобильный телефон, на который должны приходить SMS-уведомления об операциях! При смене номера мобильного телефона не забудьте незамедлительно уведомить об этом Банк. Замена номера мобильного телефона для целей уведомления клиента об операциях по банковской карте производится при личном обращении клиента (с паспортом) или подачей подписанного клиентом Заявления в Банк. SMS-уведомления позволяют вам оперативно реагировать на попытки несанкционированного доступа к счетам Вашей банковской карты.

2. Меры безопасности при использовании банкоматов.

При совершении операций в банкоматах соблюдайте следующие рекомендации:

2.1. Старайтесь пользоваться одними и теми же банкоматами, установленными в безопасных местах (например: в государственных учреждениях, отделениях банков, крупных торговых комплексах, гостиницах и т.п.), которые Вам хорошо известны. Это позволит Вам сразу определить какие-то изменения в их внешнем виде;

2.2. В случае необходимости использовать новый банкомат, выбирайте хорошо освещенный и установленный в удобном месте;

2.3. Прежде чем подойти к банкомату, осмотрите окружающее пространство. В случае нахождения поблизости подозрительных людей, воспользуйтесь другим банкоматом;

2.4. Если для прохода к банкомату используется устройство считывания карт, то для разблокировки замка никогда не требуется вводить ПИН-код. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат;

2.5. Перед использованием банкомата осмотрите его внешний вид. На банкоматах не должно быть дополнительных устройств с непонятным предназначением или наклеенных кармашков для рекламных материалов и т.п. В случае, если клавиатура или место для приема карт 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;

2.6. Не применяйте физическую силу, чтобы вставить карточку в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата;

2.7. Никогда не совершайте с банкоматом действий по совету третьих лиц, позвонивших и представившихся сотрудниками Банка или других организаций;

2.8. Будьте особенно осторожны, если кто-то посторонний предлагает Вам около банкомата помощь, даже если у Вас застряла карточка или возникли проблемы с проведением операции. Не набирайте ПИН-код на виду у «помощника», не позволяйте себя отвлечь, т.к. в этот момент мошенники могут забрать из банкомата Вашу карточку или выданные денежные средства;

2.9. Если у банкомата за Вами находится очередь, убедитесь, что никто не может увидеть Ваш ПИН-код;

2.10. При вводе ПИН-кода находитесь как можно ближе к банкомату, закройте клавиатуру второй ладонью или кошельком;

2.11. Вводите ПИН-код только после того, как банкомат попросит Вас об этом;

2.12. Если Вам кажется, что банкомат работает неправильно, нажните кнопку «отмена», заберите свою карточку и воспользуйтесь другим банкоматом. Если проблемы возникли после момента ввода запрошенной суммы, не отходите от банкомата до тех пор, пока не убедитесь в завершении операции, отказе в выдаче или в появлении на экране приглашения провести новую операцию;

2.13. После получения денежных средств, пересчитайте банкноты полистно, убедитесь в том, что банковская карта была возвращена банкоматом, дождитесь выдачи квитанции при ее запросе, положите наличность и карточку в бумажник, кошелек, сумку и т.п. и только после этого отходите от банкомата;

2.14. Если при проведении операций с использованием банковской карты в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в Банк и далее следовать инструкциям сотрудника Банка;

2.15. Если в результате какой-либо подозрительной ситуации Вам показалось, что Ваш ПИН-код стал известен посторонним людям, измените ПИН-код в банкомате Банка, либо обратитесь по телефону Горячей Линии Банка для блокировки и перевыпуска карты.

3. Меры безопасности при оплате товаров и услуг в торговых точках:

3.1. Старайтесь не терять из зоны видимости карту, которой Вы расплачиваетесь;

3.2. Сотрудник торгово-сервисного предприятия не должен долго рассматривать карту, стараясь запомнить ее реквизиты или каким-либо образом их зафиксировать (записать, скопировать, сфотографировать);

3.3. Избегайте торговых точек, в которых осуществляется видеонаблюдение зоны оплаты товаров с близкого расстояния (камера установлена на расстоянии менее 2-х метров);

Помните, что:

- операции, проведенные без ввода ПИН-кода по бесконтактной технологии в пределах лимита по таким операциям, оспорить нельзя;
- операции, подтвержденные вводом ПИН-кода, оспорить нельзя;
- никаких сведений от Вас, кроме документа, удостоверяющего личность, сотрудник торговой точки попросить не имеет права;
- следите за тем, чтобы операция оплаты всегда проходила по чипу или бесконтактным способом. За редким исключением операции по магнитной полосе не проводятся.

4. Меры безопасности при оплате товаров и услуг в интернет:

4.1. При переадресации на платежный шлюз перед вводом реквизитов карты обращайте внимание на наличие знаков 

и/или 

;

Данные технологии обеспечивают дополнительную безопасность при покупке товаров/оплате услуг через интернет с помощью карт Банка. При осуществлении указанных операций на Ваш мобильный телефон будет направлен код для подтверждения операции. Операция будет завершена только после ввода полученного кода. Данная услуга является бесплатной;

4.2. Старайтесь не «привязывать» на постоянной основе к каким-либо магазинам или сервисам данные своей карты;

4.3. В SMS-сообщении с одноразовым кодом проверьте название точки, в которой осуществляется оплата;

4.4. Помните, что операции, подтвержденные кодом из SMS-сообщения, оспариванию не подлежат. Будьте внимательны;

4.5. Внимательно проверяйте адрес ссылки платежного шлюза в строке интернет-обозревателя. Используйте только доверенные сайты, т.е. в начале строки должен стоять символ замка и адрес должен начинаться с https://.

С уважением,
ИНГ БАНК (ЕВРАЗИЯ) АО