

"О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ"

Соблюдение рекомендаций, содержащихся в данной Памятке, 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 через сеть Интернет.

Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой.

Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН-коде, CVV/CVC.

В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) 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 кредитной организации - эмитенте банковской карты.

Помните, что в случае раскрытия ПИН-кода, CVV/CVC, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц. С целью предотвращения таких неправомерных действий рекомендуется для проведения операций в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели.

В случае если имеются предположения о раскрытии ПИН-кода, CVV/CVC, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

Использование банковской карты в сети Интернет связано с повышенными рисками, в том числе, но не исключая: с риском финансовых потерь; с риском дублирования технического устройства; с риском изменения сообщений; с риском утраты (кражи) кодов доступа паролей; с риском отказа операций; с риском конфликтных ситуаций вне сферы контроля кредитной организации; с риском списания средств с карты плательщика в случае передачи кодов доступа и паролей другому лицу; с риском использования электронного средства платежа третьими лицами, без разрешения плательщика; с риском перехвата третьими лицами в каналах связи во время их использования информации о кодах доступа и паролях, сведениях о плательщике, сведениях о проведенных операциях, сведениях о получателях платежа, а также иных сведениях о плательщике.

При проведении операций через Интернет обязательно убедитесь в правильности адреса интернет-сайта, к которому Вы подключаетесь, т.к. похожие адреса могут использоваться для осуществления неправомерных действий. Внимательно проверяйте адресную строку браузера - название сайта должно быть написано без ошибок, адрес должен начинаться с HTTPS (<https://paysend.com/>).

Рекомендуется осуществлять переводы только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете). В случае если перевод 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 <https://paysend.com/>).

Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.