

**Рекомендации  
по снижению рисков осуществления (повторного осуществления) операций по переводу денежных  
средств с использованием банковской карты (реквизитов банковской карты) без добровольного  
согласия клиента**

**К операциям по переводу денежных средств, совершаемым без добровольного согласия клиента, могут относиться** операции, совершенные без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, в том числе с использованием методов социальной инженерии. **Мошенники**, используя методы социальной инженерии (представившись сотрудниками банка, оператора связи, органов внутренних дел и пр.), могут обманом вынудить клиента сообщить данные для проведения операции – номер банковской карты, ПИН-код, трехзначный код на обороте карты, коды СМС/PUSH – сообщений и осуществить с использованием таких сведений несанкционированные операции. В случае обнаружения списания денежных средств со счета необходимо незамедлительно обратиться в Банк.

Контакты банка	Головной офис ООО КБ «АРЕСБАНК» +7 (495) 795-32-88 отдел банковских карт (с 9:00 до 18:00)	Филиал «Тульский» ООО КБ «АРЕСБАНК» +7 (4872) 33-81-02, 36-33-72 операционный отдел (с 9:00 до 18:00)
При подозрении, что в отношении вас могут совершаться или совершаются мошеннические действия (получили подозрительное письмо, странный звонок или СМС/PUSH – сообщение) – незамедлительно обратитесь в ООО КБ «АРЕСБАНК»  Официальный сайт Банка <a href="https://www.aresbank.ru">https://www.aresbank.ru</a>		Контакт – центр для блокировки карт: - по России: 8 (800) 200-45-75 (круглосуточно) - за пределами России: +7 (383) 363-11-58 (круглосуточно)

**Клиентам следует руководствоваться** следующими рекомендациями по снижению рисков осуществления / повторного осуществления перевода денежных средств без добровольного согласия:

- 1 Ваша банковская карта является доступом к вашим деньгам, размещенным на счете. Храните банковскую карту / реквизиты банковской карты в недоступном для других месте и не оставляйте ее там, где посторонние лица могут скопировать номер банковской карты.
- 2 При совершении операции в торгово-сервисном предприятии требуйте проведения операции с использованием банковской карты в вашем присутствии. Страйтесь не допускать исчезновения банковской карты из поля зрения даже на незначительное время. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
- 3 При совершении операций по банковской карте в сети Интернет пользуйтесь услугами только проверенных интернет-магазинов, которые поддерживают технологии 3D-Secure (при проведении операций запрашиваются коды подтверждения из СМС/PUSH-сообщений).
- 4 Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
- 5 Перед использованием банкомата осмотрите его на наличие дополнительных устройств, несоответствующих его конструкции и расположенных в месте набора ПИН и в месте, предназначенном для приема банковских карт (например, неровно установленная клавиатура набора ПИН). В указанном случае воздержитесь от использования такого банкомата.
- 6 Не сообщайте свою персональную информацию третьим лицам. При обращении от имени Банка или иной организации по телефону, электронной почте, мессенджерам, через СМС-сообщения лиц с просьбами сообщить или передать конфиденциальные данные (номер банковской карты, ПИН-код банковской карты, трехзначный код (указанный на оборотной стороне банковской карты), коды из СМС/PUSH-сообщений (необходимые для подтверждения операций) ни при каких обстоятельствах не сообщайте данную информацию. Банк никогда не запрашивает у клиентов конфиденциальные данные.
- 7 Не записывайте ПИН-код от банковской карты, запомните его. В случае если это является затруднительным, храните его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

8	Подключите услугу СМС-информирования и контролируйте проведение операций по Вашей банковской карте.
9	Регулярно проверяйте выписку по счету банковской карты.
10	В случае изменения номера телефона, зарегистрированного в Банке, с использованием которого осуществляется доступ к сервисам Банка или к услуге СМС-информирование, незамедлительно обратитесь в Банк для изменения телефонного номера. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время. Если у сотрудников Банка будут устаревшие данные, они не смогут оперативно связаться с вами для уточнения информации в случае проведения подозрительных операций или при возникновении спорных ситуаций.
11	Если у Вас неожиданно перестала работать SIM-карта, незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как это может быть одним из признаков мошеннических действий, совершаемых в отношении Вас третьими лицами.
12	В случае утери смартфона/ мобильного телефона незамедлительно заблокируйте SIM-карту у оператора сотовой связи.
13	Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, мессенджерах, СМС/ММС-сообщениях из недостоверных источников, в том числе на известные сайты, а также загружать и устанавливать на смартфон/мобильный телефон программное обеспечение из недостоверных источников.
14	При общении с сотрудниками Банка пользуйтесь только теми телефонами, которые указаны на официальном сайте Банка <a href="https://www.aresbank.ru">https://www.aresbank.ru</a> либо на оборотной стороне Вашей банковской карты.
15	Не звоните и не перезванивайте по неизвестным телефонным номерам, указанным в СМС/PUSH – сообщениях, мессенджерах или письмах, даже если они пришли якобы от имени Банка.
16	Будьте внимательны при получении писем или СМС/PUSH-сообщений якобы от имени Банка. Основные признаки, того, что сообщение отправлено мошенниками: <ul style="list-style-type: none"> <li>- ссылка, указанная в сообщении, не содержит названия Банка, либо содержит его в искаженном виде;</li> <li>- запрашиваемые в сообщении действия требуют Вашего срочного ответа или принятия немедленного действия (ваш счет будет заблокирован);</li> <li>- содержит информацию, что на Ваш счет поступили денежные средства, которых Вы не ожидали.</li> </ul>
17	Не выполняйте действий по указанию или по рекомендациям третьих лиц, не сообщайте им результаты своих действий в банкоматах Банка (не сообщайте любую цифровую или буквенную информацию) третьим лицам, в том числе представляющимся сотрудниками правоохранительных органов, Банка России, операторами сотовой связи, работниками банков.

25 июля 2024 года вступил в силу Федеральный закон № 369-ФЗ от 24.07.2023 «О внесении изменений в Федеральный закон «О национальной платежной системе».

ООО КБ «АРЕСБАНК», как оператор по переводу денежных средств, **обязан до списания денежных средств клиента осуществлять проверку наличия признаков** осуществления перевода денежных средств без добровольного согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием (ч. 3.1 ст. 8 Федерального закона № 369-ФЗ). Признаки осуществления перевода денежных средств без добровольного согласия клиента утверждены Приказом Банка России от 27.06.2024 № ОД-1027 (далее – признаки мошенничества).

Банк отказывает клиенту в совершении операции с использованием банковской карты при выявлении признаков мошенничества, а также сообщает клиенту о возможности совершения повторной операции (на те же реквизиты и ту же сумму операции) путем направления СМС/PUSH-сообщения.

Если клиент совершает повторную операцию (на те же реквизиты и ту же сумму операции), то при отсутствии иных установленных законодательством РФ оснований Банк принимает к исполнению операцию клиента, однако, если до проведения повторной операции Банк получил от Банка России информацию, содержащуюся в базе данных Банка России ««О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента», Банк отказывает в совершении операции на срок два дня, а также сообщает клиенту о возможности совершения последующей повторной операции (на те же реквизиты и ту же сумму операции) путем направления СМС/PUSH-сообщения.

Если по истечении двух дней клиент не совершил последующую повторную операцию с использованием банковской карты (на те же реквизиты и ту же сумму операции) Банк принимает к исполнению операцию клиента, при отсутствии иных установленных законодательством РФ (ч. 3.11 ст. 8 Федерального закона № 369-ФЗ). В таком случае, Банк выполнил предусмотренные законодательством РФ меры по защите клиента от мошеннической операции и, в случае несогласия клиента с такой операцией, банк не вернет клиенту денежные средства за операцию на счет злоумышленника (ч. 3.13 ст. 8 Федерального закона № 369-ФЗ).