О 161-ФЗ и его влиянии на ваши операции

Работа Национальной платежной системы регулируется Федеральным законом № 161-ФЗ, который охватывает транзакции как физических, так и юридических лиц.
Его положения дополняются Законом № 369-ФЗ, где детально описаны действия кредитных организаций в отношении операций, признанных подозрительными или совершенных без согласия держателя счета.

Все банковские учреждения обязаны передавать информацию в Банк России о переводах, выполненных несанкционированно или под влиянием злоумышленников. Банк России, в свою очередь, тщательно проверяет эти данные и формирует специальную информационную базу.

Данные о клиентах попадают в эту базу преимущественно **двумя способами:**
• На базе обращений потерпевших: В этот раздел включаются реквизиты лиц, которые могут быть связаны с мошенническими схемами или иной незаконной деятельностью, согласно жалобам, поступившим в Банк России и другие банки.
• По информации от правоохранительных органов: Отдельный сегмент базы содержит сведения о гражданах, в отношении которых поданы заявления в полицию или ведется следствие, данные о которых поступают из МВД.

Банк России сохраняет конфиденциальность в отношении принципов формирования этой базы данных, а также состава и оснований включения в нее тех или иных реквизитов.

Причины отправки данных в Банк России

В соответствии с требованиями 161-ФЗ Банк не может сообщать подробности операций, из-за которых обслуживание ограничено.

Банк России определил шесть признаков мошеннических операций. При нахождении одного из них, Банк должен приостановить или отменить перевод.

Последствия блокировки по 161-ФЗ при приостановке или отмене операции

В случае временной приостановки транзакции банк спишет соответствующую сумму с вашего счета, но задержит ее на стадии обработки. Мы свяжемся с вами по телефону для подтверждения перевода, и при вашем согласии средства будут отправлены получателю через 48 часов. Законодательство не предусматривает возможности ускорения этого процесса.
Если в процессе звонка вы откажетесь от подтверждения операции, или же в течение 48 часов после ее первоначального подтверждения измените свое решение и сообщите об этом в банк, мы аннулируем перевод и зачислим деньги обратно на ваш счет.
Ускорение перевода невозможно. Согласно Федеральному закону № 161-ФЗ, 48-часовая пауза является обязательной, и банк не вправе ее сокращать, даже по обращению в службу поддержки.

Если операция будет окончательно отменена, перевод не состоится, и средства не будут списаны с вашего счета. В такой ситуации, если вы по-прежнему хотите осуществить платеж, рекомендуется попробовать отправить деньги на другой счет, использовать иные реквизиты получателя или использовать иной способ перевода, например, по номеру телефона. Платёж может пройти успешно, если другие реквизиты получателя еще не попали в базу данных Банка России. Предварительно узнать, какие именно реквизиты включены в эту базу, невозможно.

Ограничения при внесении данных в базу по требованию ЦБ РФ (согласно п. 11.6 ФЗ № 161)

Если ваши реквизиты будут включены в базу данных по инициативе Банка России на основании пункта 11.6 Федерального закона № 161-ФЗ:
• Денежные средства, находящиеся на ваших счетах сохраняются, а также продолжается начисление процентов по вкладам.
• В течение календарного месяца общая сумма переводов другим физическим лицам не может превышать 100 000 рублей. Этот лимит устанавливается индивидуально для каждого банка и обновляется в первый день нового месяца. Ограничение не применяется к расчетным счетам индивидуальных предпринимателей и юридических лиц.
• Отправляющий банк может временно приостановить поступление средств физическому или юридическому лицу на срок до 48 часов, либо полностью отменить такую транзакцию.
• Месячный лимит на снятие наличных в банкоматах установлен в размере 100 000 рублей, как для физических, так и для юридических лиц.
• Будет ограничена возможность оформления новых банковских продуктов.

Как только ваши реквизиты будут исключены из базы данных Банка России, вы сможете вновь в полной мере пользоваться всеми банковскими продуктами.

Ограничения при включении данных в базу по запросу МВД (согласно п. 11.7 ФЗ № 161)

В ситуации, когда информация о клиенте попадает в базу Банка России на основе данных, полученных от Министерства внутренних дел, банк примет более строгие меры:
• Будут немедленно отключены ваши банковские карты, а также заблокирован доступ к мобильному приложению и личному кабинету.
• Невозможно будет расплачиваться картами, совершать платежи по QR-кодам, осуществлять переводы, снимать наличные в банкоматах, а также использовать любые функции приложения и личного кабинета.

! Денежные средства на вашем счете останутся в сохранности, и вы по-прежнему сможете получать входящие переводы.

После того как реквизиты клиента будут удалены из базы данных Банка России, все ранее заблокированные функции и продукты банка восстановятся в полном объеме.

Рекомендации по исключению данных физического или юридического лица из базы Банка России

Чтобы подать запрос на удаление ваших сведений или информации о вашей организации из реестра Банка России, воспользуйтесь официальным сайтом.

1. Откройте онлайн-приемную Банка России. Прокрутите страницу до конца и найдите кнопку «Направить обращение».
2. На появившейся странице выберите опцию «Исключить данные из базы данных Банка России о случаях и попытках совершения операций без согласия клиента». Она может быть расположена на сером фоне или в разделе «Информационная безопасность».
3. Продолжите, нажав «Перейти к оформлению обращения» после прокрутки страницы вниз.
4. Укажите ваш статус: являетесь ли вы физическим или юридическим лицом.

Для физических лиц: воспользуйтесь кнопкой «Госуслуги» для входа через подтвержденную учетную запись.
Для юридических лиц: внесите все необходимые сведения о вашей компании вручную.

Завершив этот этап, нажмите «Продолжить».

5. В текстовом поле «Текст обращения» четко и свободно опишите причину вашего обращения.
6. Заполните остальные поля, указав название вашего банка, номер карты или счета, данные паспорта, ИНН и другую релевантную информацию. Это ускорит рассмотрение вашего запроса Банком России. После заполнения нажмите «Далее».
7. Внимательно проверьте все введенные данные на корректность. Если всё верно, нажмите «Отправить обращение». В случае необходимости внесения изменений, выберите «Редактировать».

! Ожидайте ответа от Банка России в течение 15 рабочих дней.

Рекомендации по снижению рисков повторного осуществления переводов денежных средств без добровольного согласия

1. Всегда тщательно проверяйте отправителя сообщений (SMS, электронных писем, мессенджеров) и ссылки, прежде чем переходить по ним. Мошенники часто маскируются под банки, государственные органы или известные компании.
2. Будьте внимательны к звонкам от неизвестных лиц, представляющихся сотрудниками банка или правоохранительных органов, особенно если они требуют конфиденциальные данные (пароли, коды из SMS, полные данные карт) или просят перевести деньги на "безопасный счет". Помните, что сотрудники банка никогда не запрашивают такие данные.
3. Используйте сложные и уникальные пароли для всех онлайн-банкингов и финансовых приложений. Регулярно меняйте их.
4. Активируйте двухфакторную аутентификацию (2ФА) везде, где это возможно (например, вход по паролю + код из SMS/приложения-аутентификатора).
5. Никогда не делитесь своими логинами, паролями, PIN-кодами и кодами подтверждения из SMS с третьими лицами, даже если они представляются сотрудниками банка.

6. Подключите SMS-уведомления или push-уведомления о каждой операции по вашим картам и счетам. Это позволит мгновенно реагировать на любые подозрительные действия.
7. Регулярно проверяйте выписки по своим банковским счетам и картам. При обнаружении любых подозрительных операций немедленно свяжитесь с банком.
8. При подозрении на несанкционированный доступ к вашим счетам или совершенную мошенническую операцию немедленно заблокируйте карту (через мобильное приложение, личный кабинет или по телефону горячей линии) и свяжитесь с банком.
9. Сохраняйте все доказательства мошенничества (скриншоты переписки, данные о звонках и т.д.) для возможного обращения в правоохранительные органы.