**О возможности установления гражданином запрета (ограничения) на онлайн-операции, в том числе на заключение кредитными организациями с ним договоров потребительского займа (кредита), в целях предупреждения мошеннических действий со стороны третьих лиц**

Пунктом 7.1. Положения «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», разработанного Центральным банком Российской Федерации от 17 апреля 2019 г. № 683-П определено:

«В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) договора об использовании электронного средства платежа, на основании их заявлений устанавливают в отношении операций, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций через информационно-телекоммуникационную сеть «Интернет», ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе видов операций».

Центробанк обязал банки с 1 октября 2022 года предоставить клиентам возможность собственноручно накладывать запрет на онлайн-операции и ограничивать их параметры (как при кредитовании, так и при денежных переводах).

**Самозапрет на кредиты, что это?**

Это ограничение, которое банк по заявлению клиента накладывает на операции, осуществляемые с помощью удаленного доступа через интернет. Запретить можно как отдельно кредитование, так и другие банковские операции или установить максимальную сумму.

Принят федеральный закон, по которому граждане могут устанавливать самозапрет на выдачу кредитов, который начнет действовать с 1 марта 2025 года. Можно будет устанавливать запрет на заключение договоров потребительского займа с банками и микрофинансовыми организациями (МФО). Гражданам дадут право подать во все квалифицированные бюро кредитных историй заявление через единый портал госуслуг, а также запросить информацию о наличии в кредитной истории сведений о таком ограничении. К заявлению нужно будет прикрепить данные СНИЛСа.

Снять запрет можно будет в любое время, но взять кредит получится только после того, как данные попадут в кредитную историю. Депутаты считают, что такой «период охлаждения» позволит исключить риск мошенничества с одномоментным снятием запрета и заключением кредитного договора.

**В каких случаях стоит оформить самозапрет на кредит?**

Категорий людей, которым рекомендуют оформить такой самозапрет, нет. В настоящее время юристы рекомендуют делать это лично, в присутствии сотрудника банка и самого клиента, с обычной подписью (целесообразно написать заявления о запрете во все крупные банки, а как минимум в те, где вы когда-либо обслуживались по дебетовой карте, кредитной карте, кредиту.

**Как оформить самозапрет на кредиты через «Госуслуги»?**

С 1 марта 2025 года самозапрет на кредиты можно будет выставить на «Госуслугах», с 1 сентября 2025 года — в МФЦ. Эти данные автоматически попадут в бюро кредитных историй. Банки, которые запрашивают информацию в бюро, увидят выставленные ограничения на кредитование. Пока эта опция недоступна.

**Можно ли оформить самозапрет через банки, микрофинансовые и другие организации?**

Пока это единственный вариант, и он уже вступил в силу и действует с октября 2022 года.

В отдельных банках можно написать заявление о запрете онлайн-кредитования конкретно в них. Такая опция есть практически во всех крупных банках, но есть те, которые будут против (к ним необходимо относится скептически, т.к. они не соответствует рекомендациям Центробанка что повышает риски заемщика).

Условия и порядок оформления такого запрета сегодня устанавливает банк.

Аналогичные запреты можно направить и в микрофинансовые организации, но технически сделать это будет сложнее т.к. их слишком много, зарегистрированы они в разных регионах, а о существовании некоторых можно просто не знать.

**Можно ли снять самозапрет?**

Да. Можно запретить выдавать кредиты на свое имя, потом отозвать запрет, потом запретить снова. Центробанк никак не ограничивает количество таких процедур.

**Плюсы и минусы самозапрета на кредиты.**

Плюс очевиден — самозапрет на кредиты поможет защититься от мошенников. А возможно, и от спонтанных покупок — кредиты выдаются онлайн за несколько минут. Но если придется ехать в банк, чтобы снимать самозапрет, велик шанс передумать.

Минус только в том, что если вы сами соберетесь взять кредит, то придется потратить время и сходить в отделение банка. Большой проблемы в этом нет, особенно если вы живете в городе, где есть отделение банка. Но если вы проживаете в маленьком городке, где отделений нет и не хочется никуда ехать, то это проблематично.

В принципе, онлайн-кредит — это удобно, но система будет хороша только тогда, когда каждый гражданин будет обладать своей квалифицированной электронной цифровой подписью. Не простой, а именно квалифицированной, как, например, у судей.

**Обезопасит ли самозапрет полностью от мошенников?**

Полностью — нет, однако он существенно усложнит мошенникам задачу и как минимум защитит от некоторых схем и от потери крупных сумм.

**Как обезопасить себя, пока закон не начал действовать?**

Если вы хотите оформить именно самозапрет на кредитование или переводы, это можно сделать непосредственно в банке. Конечно, потребуется время, чтобы обратиться во все кредитные организации, но для начала можно подать заявления в банки, услугами которых вы когда-либо пользовались.

Сейчас у некоторых банков есть специальная последовательность действий для онлайн- кредитования, чтобы избежать мошенничества. Например, счет заемщика могут заблокировать, если он пытается сразу же после получения кредита снять или перевести деньги. Для разблокировки счета придется связаться с банком или посетить отделение лично.

**Рекомендации:**

Юристы советуют раз в год или полгода запрашивать отчет из бюро кредитных историй. Это уже сейчас можно сделать на «Госуслугах» — через сайт заказать выписку из всех БКИ, в которых содержится информация о клиенте.

Также можно периодически проверять себя через систему судебных приставов на сайте ФССП. Достаточно указать ФИО, дату рождения и выбрать регион, по которому будет производиться проверка.

Не пересылайте никогда фотографии паспорта — в некоторых случаях займ могут оформить по фото или копии документа. Если куда-то нужно отправить данные, лучше не полениться и переписать их. Если вам стало известно, что эти данные уже куда-то попали целесообразно менять паспорт. При этом, если паспорт украли или вы его потеряли, следует обратиться в полицию.

Возьмите там справку о том, что паспорт утерян, с указанием даты. Если паспорт попадет в руки мошенников, эта справка будет основным доказательством того, что кредит или займ брали не вы. Иногда мошенникам достаточно только паспортных данных, поэтому их тоже стоит беречь. Не сообщайте данные по телефону или в соцсетях, не вводите данные на непроверенных и незащищенных сайтах (в адресной строке должно быть изображение закрытого замка). В случае звонка «из банка» не разговаривайте со звонящими — общайтесь в чате поддержки на официальном сайте или в приложении либо перезвоните в банк самостоятельно.

**Памятка о наиболее распространенных способах совершения IT-преступлений, рисков хищений с применением цифровых технологий и методах защиты от них**

Злоумышленник представляется сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета, используя IP-телефонию звонит потерпевшему с подменных номеров и информирует гражданина о подозрительных финансовых операциях по его банковскому счету, попытках оформления кредита, перевода денежных средств с его счета, либо сообщает о розыске, задержании преступников, совершающих хищения денежных средств с расчетных счетов граждан, при этом извещает о необходимости соблюдения некой «тайны следствия».

Далее, используя методы психологического манипулирования и пользуясь доверчивостью, злоумышленник вынуждает потерпевшего сообщать персональные данные, сведения о финансовом состояния, наличии автотранспорта в собственности. Затем, находясь под психологическим воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета.

Злоумышленник, маскируясь под представителя оператора связи, убеждает потенциальную жертву посягательства, что срок действия sim-карты для использования мобильной связи истекает. Для продления ее работы необходимо сообщить код из присылаемого SMS-сообщения. Такое действие обеспечивает возможность подключения переадресации звонков и SMS-сообщений на другой телефонный номер и получение доступа к онлайн-банкингу, социальным сетям и мессенджерам потерпевшего для входа по номеру телефона.

Совершение посягательства под предлогом оказания содействия родственнику, якобы попавшему в дорожно-транспортное происшествие или задержанному правоохранительными органами. Введенный в заблуждение человек передает денежные средства прибывшему к нему курьеру, который в дальнейшем перечисляет полученные денежные средства на указанные мошенниками банковские счета (при этом оставляя себе определенный процент средств).

Еще одной распространенной мошеннической схемой остается предлог дополнительного заработка, участия в торгах на бирже, а также инвестирования в различные ценные бумаги. Граждан заманивают яркими вывесками, наименованиями, созвучными с названиями крупных нефтегазодобывающих компаний и холдингов, так называемыми «исключительными» предложениями и возможностью получения высокого дохода, в том числе за короткий промежуток времени. Попавшего под воздействие указанных факторов человека вынуждают вносить крупные суммы денежных средств, без возможности их вывода в дальнейшем.

Совершение мошеннических действий с использованием популярных торговых интернет-площадок объявлений о купле-продаже различного имущества или оказания услуг путем:

Размещения «фиктивного» объявления о продаже товара по цене значительно ниже рыночной. Как правило, переписка между покупателем и мошенником ведется на торговой площадке либо с использованием популярных интернет-мессенджеров. В ходе общения мошенник входит в доверие и вынуждает потерпевшего оплатить товар полностью либо внести определенную предоплату путем электронных переводов. После оплаты контакты с покупателем как правило прекращаются, его блокируют, объявление удаляют.

Хищения денежных средств под предлогом приобретения товара у потенциальной жертвы. В данном случае переписка между продавцом и мошенником также ведется с использованием сообщений на сайте, либо с использованием мессенджеров. Продавца убеждают направить товар популярными интернет-сервисами доставки, в том числе используемыми на торговых площадках, сообщая, что товар оплачен, и для получения денежных средств необходимо перейти по ссылке, которую присылают на телефон продавца.

После перехода по ссылке продавец попадает на фишинговый сайт, аналогичный официальному сайту торговой площадки, где вносит свои персональные данные, реквизиты банковской карты и необходимую сумму. После нажатия на «окно» «Получить деньги», денежные средства списываются с расчетного счета продавца. В дальнейшем мошенники убеждают продавца, что произошел некий сбой и для возврата денежных средств необходимо обратиться в службу поддержки, перейдя по еще одной присылаемой ссылке. Продавец, перейдя по ссылке, вновь попадает на фишинговый сайт, где повторно указывает свои данные, реквизиты карты и сумму, якобы необоснованно списанную. После нажатия на «окно» «Получить деньги» с расчетного счета продавца повторно списываются денежные средства.

Аналогичным способом совершается хищение денежных средств через сервис по поиску попутчиков: мошенники размещают объявления с предложением услуги по пассажирским перевозкам. Когда пользователь откликается на объявление, мошенник в чате официального сайта поиска попутчиков просит его связаться с ним через популярный мессенджер по определенному номеру телефона. Затем, в ходе переписки клиенту предлагают оплатить поездку заранее и скидывают ему для этого ссылку на фишинговый сайт для оплаты. После перехода на сайт, пользователь вводит реквизиты своей банковской карты, далее денежные средства списываются на счет мошенникам.

Распространение получила схема хищения денежных средств с использованием социальных интернет-сетей. Якобы от имени потерпевшего его знакомым, друзьям, родственникам приходит сообщение с просьбой одолжить денежные средства. Также злоумышленники с использованием популярных мессенджеров рассылают сообщение о сборе денежных средств на лечение больного ребенка, похороны и т.д.

Действует преступная схема с оформлением кредита в микрофинансовых организациях без ведома потерпевшего. Хищение осуществляется путем перебора сим-карт для поиска активного аккаунта заемщика и использование личного кабинета лица, ранее оформлявшего в микрофинансовых организациях заем.

Еще одним способом остается совершение противоправных деяний под предлогом получения возврата (компенсации) денежных средств за ранее приобретенные биологически активные добавки (БАДы). Мошенники, представляясь сотрудниками правоохранительных органов, в телефонном разговоре с потерпевшим сообщают, что задержали преступников, занимавшихся ранее продажей некачественных пищевых добавок. Для получения компенсации необходимо оплатить налог, открыть счет, совершить транзакцию и т.п. В результате граждане, рассчитывая получить компенсацию, перечисляют мошенникам денежные средства, сумма которых превышает сумму обещанной компенсации.

**Чтобы не оказаться жертвой мошенников необходимо знать следующее:**

* сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них имеются ваши данные;
* хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;
* не сообщать пин-код третьим лицам;
* лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка;
* внимательно читайте СМС сообщения, приходящие от банка;
* никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;
* сотрудники банка никогда не попросят вас пройти к банкомату;
* никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;
* в сети «Интернет» не переходите по ссылкам на неизвестные сайты.