РостФинанс

Оглавление

Уважаемые клиенты!

Уровень преступности в сфере информационно-коммуникационных технологий остаётся стабильно высоким.

Разновидность преступлений в условиях современного мира весьма обширна: от телефонных мошенничеств, фишинг-ресурсов, криптопирамид, DoS-атак на предприятия критической информационной инфраструктуры, незаконной торговли персональными данными до нескончаемо разных преступлений.

Одним из самых распространённых видов преступлений является использование мошенниками банковских счетов граждан для переводов денежных средств. Это могут быть переводы денежных средств без добровольного согласия клиентов или вовлечение в мошеннические схемы обманом, угрозами или уговорами, в результате которых клиент становится «дропом» или «дроппером».

В настоящей памятке мы подробно расскажем, какие у клиентов есть права, обязанности и ответственность перед законодательством в каждой из этих ситуаций.

ПЕРЕВОДЫ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ: КРАТКИЙ ОБЗОР ПРАВ И ОБЯЗАННОСТЕЙ КЛИЕНТОВ

Денежные переводы чаще всего совершаются посредством использования банковских карт и интернет-банка (онлайн-банк), включающего и мобильное приложение. Эти инструменты относятся к электронным средствам платежа (ЭСП).

Законодательством для банка и клиента установлен ряд прав и обязанностей, от соблюдения или несоблюдения которых зависит, будут ли клиенту возвращены суммы, похищенные с его счёта, или нет (п. 19 ст. 3, ст. 9 Федерального закона от

27.06.2011 N161-ФЗ «О национальной платежной системе» (далее «Закон №161-ФЗ»).

Основная обязанность банка – информировать клиента о каждой операции, совершённой с использованием ЭСП, путем направления клиенту уведомления (далее – уведомление об операциях) в порядке, установленном договором с клиентом (ч. 4 ст. 9 Закона N161-ФЗ).

При выявлении банком операций, соответствующих признакам перевода денежных средств без согласия клиента, банк должен приостановить использование клиентом банковской карты и предоставить ему соответствующую информацию. Указанные признаки устанавливаются Банком России и размещаются на его официальном сайте (ч. 5.1, 5.2 ст. 8, ч. 9.1 ст. 9 Закона N161-ФЗ; признаки, утв. Приказом Банка России от 27.09.2018 N ОД-2525).

При этом банк обязан в день приостановления использования клиентом банковской карты предоставить ему соответствующую информацию (уведомление) с указанием причины приостановления. Такие уведомления направляются в порядке, установленном договором (ч. 9.2 ст. 9 Закона N161-ФЗ).

Способы направления уведомлений об операциях, используемые банками, различны. Это могут быть и СМС-уведомления, и рассылка по электронной почте, и информирование в интернет-банке. При этом хотя бы один из способов информирования должен быть бесплатным для клиента.

Основная обязанность клиента – уведомить банк в случае утраты ЭСП и (или) его использования без согласия клиента. При этом клиент обязан направить в банк указанное уведомление (далее – уведомление о несогласии) незамедлительно после обнаружения факта утраты ЭСП и (или) его использования без согласия клиента, но не позднее дня, следующего за днём получения от банка уведомления об операциях (ч. 11 ст. 9 Закона N161-ФЗ).

Способ информирования устанавливается договором. На практике чаще всего используется звонок в Контакт-центр банка с последующим представлением уведомления о несогласии в письменной форме.

День получения от банка уведомления об операциях – это не день, когда вы фактически его прочитали, а день, определённый в качестве такового договором. В договоре обычно указывают, что вы считаетесь получившим уведомление в день его направления банком установленным договором способом, например, по

указанному вами номеру мобильного телефона. Если вы вовремя не прочитали уведомление, это ваша вина.

Клиент имеет право на возмещение от банка суммы несанкционированных операций, совершенных с использованием ЭСП, в следующих случаях (ч. 12, 13, 15 ст. 9 Закона N161-ФЗ):

1) если банк не направлял вам уведомления о совершённых операциях, он обязан возместить вам суммы операций, которые были совершены без вашего согласия (далее также – несанкционированные операции) и о которых вы не были банком проинформированы. Соответственно, в данном случае срок, установленный для направления вами уведомления о несогласии, не применяется;
2) если банк надлежащим образом направлял вам уведомления о совершённых операциях и вы вовремя представили в банк уведомление о несогласии, банк обязан возместить вам суммы несанкционированных операций, совершенных после предоставления вами уведомления о несогласии;
3) если банк надлежащим образом направлял вам уведомления о совершенных операциях и вы вовремя представили в банк уведомление о несогласии, банк обязан возместить вам суммы несанкционированных операций, совершенных до момента представления вами указанного уведомления о несогласии, но только в том случае, если не сможет доказать, что вы сами нарушили порядок использования ЭСП, из-за чего и произошли несанкционированные операции.

Обратите внимание! С 25 июля 2024 года вступает в законную силу новая редакция Закона N161-ФЗ.

Изменение Закона N161-ФЗ направлено на модернизацию не только существующего механизма противодействия хищению денежных средств, но и действующего механизма возврата уже списанных со счетов клиентов денежных средств.

Банк будет обязан осуществить проверку наличия признаков осуществления перевода денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, до момента списания денежных средств клиента (в случае совершения операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платёжной системы Банка России)

либо при приёме к исполнению распоряжения клиента (при осуществлении перевода денежных средств в иных случаях).

При выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента, банк приостанавливает приём к исполнению распоряжения клиента на 2 дня. Если операция по переводу выполняется с использованием платёжных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России, то банк отказывает в совершении соответствующей операции (перевода).

После введения ограничения на перевод банк обязан будет сообщить клиенту:

- о приостановке и отказе в выполнении операции по переводу денежных средств;
- о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента;
- о возможности клиента подтвердить распоряжение не позднее одного дня, следующего за днём приостановления банком приёма к исполнению указанного распоряжения, или о возможности совершения клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее – повторная операция), в случае отказа банка по переводу денежных средств с использованием платёжных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платёжной системы Банка России.

При неполучении от клиента подтверждения распоряжения указанное распоряжение считается не принятым к исполнению, а при осуществлении действий по совершению клиентом повторной операции способом, не предусмотренным договором, операция считается несовершённой. Однако, если банк получил информацию от Банка России о рисках данного перевода, банк приостанавливает приём к исполнению подтвержденного распоряжения клиента на 2 дня. При этом банк обязан незамедлительно уведомить клиента о приостановлении перевода или об отказе в переводе с указанием причины такого приостановления (отказа) и срока такого приостановления, а также о возможности совершения клиентом последующей повторной операции.

Если банк, несмотря на имеющуюся у него информацию от Банка России, содержащуюся в базе данных о случаях и попытках осуществления переводов

денежных средств без добровольного согласия клиента (далее – база), выполнил перевод денег, то клиент вправе требовать возмещения суммы перевода в течение 30 дней, следующих за днём получения банком соответствующего заявления клиента. В тот же срок возмещение производится, если банк не проинформировал клиента о рискованности выполняемой операции, совершённой без добровольного согласия клиента.

В случае нахождения электронного средства платежа в базе, а также сведений федерального органа исполнительной власти в сфере внутренних дел о совершённых противоправных действиях банк обязан выполнить приостановку использования клиентом электронного средства платежа.

После приостановления использования клиентом электронного средства платежа клиент вправе подать заявление в Банк России, в том числе через обслуживающий банк об исключении сведений либо вообще его данных из базы, т.е. о разблокировке. В случае наличия у банка оснований полагать, что включение сведений, относящихся к клиенту и (или) его электронному средству платежа в базу является необоснованным, такой банк вправе самостоятельно (без участия клиента) направить в Банк России мотивированное заявление об исключении сведений.

Мотивированное решение об удовлетворении или об отказе в удовлетворении заявления клиента принимается в срок, не превышающий 15 рабочих дней. Решение об отказе в удовлетворении таких заявлений клиент вправе обжаловать в суд в соответствии с законодательством Российской Федерации.

ОБ ОТВЕТСТВЕННОСТИ ВЛАДЕЛЬЦЕВ ДЕНЕЖНЫХ СЧЕТОВ («ДРОППЕРОВ») В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИХ В МОШЕННИЧЕСКОЙ СХЕМЕ

Граждане всё чаще теряют свои деньги не без помощи так называемых «дропперов», т.е. лиц, на счета которых похищенные мошенническим способом средства переводятся для последующего обналичивания.

«Дропы» («дропперы»), как правило, самостоятельно предоставляют свои данные мошенникам для открытия счетов, чтобы уводить по цепочке похищенные деньги, затрудняя выход на изначального злоумышленника, или делают это через свои счета.

Использование услуг «дропов» для обналичивания криминальных доходов может быть расценено как легализация, за совершение которой наступает уголовная

ответственность, предусмотренная статьей 174 Уголовного кодекса Российской Федерации (совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом). Максимальное наказание — лишение свободы на срок до 7 лет.

Статьей 187 УК РФ предусмотрена уголовная ответственность за неправомерный оборот средств платежей, под которым понимается изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приёма, выдачи, перевода денежных средств. Максимальное наказание — лишение свободы на срок до 7 лет.

С лиц, незаконно завладевших денежными средствами, на основании ст. 1102 Гражданского кодекса Российской Федерации в судебном порядке может быть взыскана вся сумма похищенных у потерпевших денег.

При рассмотрении в суде дела истец (потерпевший) должен доказать факт приобретения или сбережения имущества ответчиком («дроппером»), а тот, наоборот, подтвердить наличие законных оснований для приобретения или сбережения такого имущества либо наличие обстоятельств, при которых неосновательное обогащение в силу закона не подлежит возврату.

Утрата карты сама по себе не лишает клиента банка прав в отношении средств, находящихся на банковском счете, и возможности распоряжаться этими деньгами, поэтому доводы ответчиков («дропперов») о потере карты судами отклоняются, решения выносятся в пользу потерпевших. Более того, даже заявленные ими доводы о передаче данных о счёте третьим лицам не рассматриваются как достаточное основание для отказа в удовлетворении иска, поскольку в этих случаях фактически подтверждается нарушение условий банковского обслуживания и неправомерное завладение чужими денежными средствами.

Таким образом, обозначенная судебная практика позволяет потерпевшим от преступлений в сфере информационно-телекоммуникационных технологий, даже при неустановлении подлежащего привлечению к уголовной ответственности лица, эффективно защищать свои права и возмещать причинённый ущерб.

Следует отметить, что граждане, предоставляя свои персональные данные, рискуют также оказаться участниками схем продажи оружия или наркотиков, передачи/получения взяток, указанные данные могут быть использованы для регистрации фиктивной фирмы, оформления кредита и т.д.

КАК ИЗБЕЖАТЬ ВЗАИМОДЕЙСТВИЯ С МОШЕННИКАМИ

Не соглашайтесь как-либо помогать незнакомым людям у банкоматов. Если банкомат расположен в офисе кредитной организации, позовите сотрудника банка для этих целей. Если банкомат стоит в торговом центре или ещё где-то, вежливо откажите собеседнику, предложив ему позвонить на горячую линию банка.

Не соглашайтесь на предложения лёгкого заработка. Даже если подобное предложение поступило от вашего друга или знакомого — вас могут использовать в преступных целях, а друг может не знать о том, что он участник нелегальной схемы и привлекает вас к незаконным действиям.

Не продолжайте общение с потенциальными работодателями, если вакансия вызывает у вас сомнение. Как вариант — уточните официальное название компании и адрес её сайта и перезвоните на номер, указанный на сайте. Также посмотрите отзывы о компании. Если их нет, это тоже «звоночек», даже если у компании есть сайт и она представлена на популярных рекрутинговых порталах.

Не откликайтесь на предложения незнакомцев в соцсетях и мессенджерах. Чаще всего злоумышленники ищут дропперов именно там — либо заводят непринуждённый разговор для знакомства, либо сразу предлагают работу с лёгким заработком. Конечно, можно уточнить детали такой работы, а вот выполнять какие-либо задания и просьбы не стоит.

Самостоятельно перезванивайте в свой банк при любом подозрении. Если вам поступил звонок якобы от вашего банка, но разговор идёт о странных вещах или каким-либо образом вас смущает, уточните, чего от вас хотят, повесьте трубку и перезвоните по номеру банка, указанному на вашей карте. Сотруднику Контакт-центра расскажите все детали поступившего звонка, и он скажет вам, действительно ли звонил банк или это был злоумышленник, а также посоветует, как уберечь себя от подобных мошеннических атак и что делать дальше.