Ассоциация в области социальной помощи, науки, культуры, охраны здоровья граждан, здорового образа жизни, интеллектуального развития личности, охраны окружающей среды «Социальное сотрудничество»

БИБЛИОТЕЧКА ДЛЯ ДОМА

ЭКОЛОГИЯ ФИНАНСОВ

115 ФЗ?

Санкт-Петербург
2022

Собираем библиотечку для дома. В этой серии рассмотрим инструменты финансового планирования.
По просьбам и обращениям Членов Ассоциации на массовые трудности в понимании того, что делать и куда обращаться, подготовлено специалистами Росфинмониторинга, правоохранительных органов и банковскими специалистами в области ПОД/ФТ/ФРОМУ

Ассоциация «Социальное сотрудничество»,
+7 (812) 718-59-23
info@soc-part.ru
191180, город Санкт-Петербург, Большой Казачий переулок,
дом 11 литер а, помещение 48
Сайт http://alf.spb.ru/

Содержание

Что такое 115-ФЗ

Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», принят в 2001 году. За два десятилетия в закон вносились многочисленные поправки: одни нормы утрачивали силу, другие — вводились в действие.

Цель настоящего закона заключается в создании и работе правового механизма, противодействующего отмыванию доходов, финансированию террористической и экстремистской деятельности, а

также распространения оружия массового поражения.

Под действие ФЗ подпадают:

- Граждане — физические лица, занимающиеся и не занимающиеся частной практикой.
- Иностранные граждане и лица без гражданства.
- Организации, работающие с денежными средствами и имуществом.
- Юридические лица.
- Индивидуальные предприниматели.
- Иностранные организации, действующие без образования юрлица.
- Государственные и муниципальные органы.

Федеральный закон обязывает организации, работающие с денежными средствами, следить за движением денежных масс, вычисляя подозрительные и незаконные операции. Главным регулятором в сфере финансового надзора является — Росфинмониторинг. Исходя из этого, на вопрос, может ли банк заблокировать счет физического лица, ответ один — может, и под контроль подпадают банковские карты, вклады, текущие счета физлиц.

По каким причинам блокируется счет физического лица

Кредитные и прочие организации, работающие с денежными средствами, обязаны анализировать операции своих клиентов на подозрительность.

Критерий подозрительности — достаточно неопределенный и не очевидный момент, так как подозрительной может быть признана практически любая операция.

При этом закон запрещает банкам и некредитным финансовым организациям разглашать информацию о планируемых мерах по отношению к конкретному

клиенту. Блокировка счета физического лица производится без предварительного уведомления.

Это ключевой момент: банк может проинформировать клиента только после принятия в его отношении конкретных мер. До блокировки счета или расторжения договора вклада клиент о проводимых банком мероприятиям не оповещается. Объективные причины блокировки счета физического лица:

- Операции по обналичиванию денежных средств — незаконный перевод безналичных денег в наличные.
- Запутанные схемы расчетов.
- Сокрытие истинных целей и участников сделок — в банковском сегменте это принято называть «транзит».
- Незаконный вывод денежных средств за границу Российской Федерации.
- Финансирование или причастность к террористической и (или) экстремистской

Для блокировки счета или для наложения ограничений на совершение определенных операций специалисту банка (иной организации) достаточно увидеть в операции признаки одного из нарушений, приведенных

в списке. Если уполномоченному сотруднику покажется подозрительность операции, счет будет заблокирован. То есть, нарушения, как такового, может и не быть. Именно поэтому критерий подозрительности операций — условное значение, которое часто зависит от человеческого фактора.

Что делать в случае блокировки счета

Банк оповещает клиента о предпринятых в отношении его счета мерах по факту их принятия. Как правило, банк связывается с клиентом по телефону или в смс-сообщении, реже — по электронной почте.

В случае блокировки счета вариант решения проблемы один — клиент доказывает банку, что совершенная им операция (операции) не преследовала цель отмывания доходов и (или) финансирования террористической деятельности.

Сложность заключается в том, что полного перечня документов, подходящего под каждый случай, — не существует. Каждый случай рассматривается банками индивидуально, поэтому клиент в обозначенный срок предоставляет данные, указанные специалистом организации.

Документы должны подтверждать законность происхождения денежных средств, а также экономический смысл совершенной операции. Ими могут быть: договоры купли-продажи, чеки,

накладные, квитанции, листы, счета, арендные соглашения, и прочее. Пока клиент не предоставит в банк документальные расчетные данные, ограничения со счета не снимаются.

Как передать в банк подтверждающие документы

Если заблокировали счет в банке, клиент получает сообщение, в котором указывается на перечень подтверждающих документов и на способ их отправки в банк. Если клиент проживает (находится) в городе, в котором базируется региональное управление банка (иной организации), документы предоставляются лично. В остальных случаях допускается:

- Отправка копий по электронной почте.
- Отправка документов по Почте России.

Если подтверждающих документов нет в наличии, либо на их сбор клиенту требуется время, об этом необходимо сообщить в банк. Кредитные организации не заинтересованы в потере своих клиентов, поэтому для снятия ограничений со счета может быть найдено альтернативное решение.

Как подстраховаться от блокировки текущего счета (карты)

Физические лица, не занимающиеся предпринимательской деятельностью или частной практикой (нотариусы, адвокаты, арбитражные управляющие, частные детективы, охранники, и

другие), открывают в банке текущие счета, карты, вклады. Каждый из этих счетов, либо все одновременно, могут быть заблокированы банком на неопределенный срок.

Кредитные организации на своих официальных сайтах размещают информацию (памятку), которая помогает клиентам избежать возможной блокировки счетов.

Действия, которые не рекомендуется совершать, в процессе использования личного счета:

- Переводы через счет денег, к которым клиент не имеет никакого отношения — не соглашаться на просьбы друзей и знакомых, особенно, если речь идет о крупных суммах.
- Передача данных счета (карты) третьим лицам — счет может использоваться для транзита (сокрытия экономического смысла) по операции.
- Использование карты или счета для незаконной предпринимательской деятельности.
- Участие в качестве директора организации — в случае, если реальная работа в качестве директора не планируется (подставное лицо).
- Частое снятие больших сумм наличных со счета — можно и нужно стараться больше работать с безналичной формой оплаты.

Если гражданин начинает заниматься предпринимательской деятельностью, то ему запрещено пользоваться картами и счетами для принятия платежей, которые он оформлял, будучи физическим лицом. В этих целях оформляется бизнес-карта для ИП и открывается расчетный счет.

Избежать блокировку получится при соблюдении этих элементарных правил. Следует помнить, что банк выполняет предписания законодательства, и за нарушения требований 115-ФЗ в отношении участников рынка предусмотрены достаточно жесткие санкции, вплоть до отзыва банковской лицензии.

Как осуществляется мошенничество по телефону

Основой мошеннических схем служит персональная информация, полученная на нелегальном рынке баз данных интернет-магазинов, финансовых учреждений, государственных структур. Мошенники усложнили методы своей работы.

очередную жертву, чтобы убедить её перевести деньги, соблазняя финансовой выгодой и даже предлагая некую должность с высокой оплатой. И ради этого устраивают видеособеседования с потенциальным «работодателем». Каждый день появляются всё новые методики, но средства борьбы с преступниками тоже не стоят на месте.

Можно рассмотреть основные виды телефонного мошенничества:

1. Мошенничество с банковскими картами и счетами

- Платежная карточка, безусловно, удобная и полезная вещь. Но крайне соблазнительная для криминальных воздействий. Весьма распространена схема воровства «на доверии». Так, телефон из объявления в интернете или СМИ о продаже любого имущества немедленно попадает в поле зрения мошенников. И владельцу звонит некий

«потенциальный покупатель», готовый платить, не торгуясь, но только на карту.

Для этого он просит сообщить её номер, срок действия, CVV-код с обратной стороны карты. И SMS-код из сообщения банка о проведённой операции. Даже если не удаётся получить весь набор информации, недостающие данные восполняются квалифицированными хакерами. И карточный счёт не пополняется, а опустошается путём перевода наличности на некий электронный кошелек, который немедленно исчезает из сети после вывода средств с него.

2. Звонки от «службы безопасности» банков

- Не менее распространены звонки из «службы безопасности банка-эмитента платежной карты» о совершённой подозрительной операции или сбое в программном

обеспечении, который привел к потере средств. Для восстановления счёта и возврата денег якобы необходимы вышеперечисленные данные.

Для защиты от подобных инцидентов рекомендуют установить определенные программы, замаскированные под известные сервисы. Но на самом деле эти утилиты отправляют мошенникам коды доступа к счетам, полностью развязывая преступникам руки.

3. Звонки от сотрудников правоохранительных органов и государственных служб.

- Особенно циничны звонки из правоохранительных органов, якобы расследующих случаи мошенничества по телефону. Цель та же самая — усыпить бдительность и выманить нужную информацию. На фоне пандемии активизировались мошенники, которые представляются работниками Роспотребнадзора или Пенсионного фонда с сообщениями о новых социальных выплатах. Но для их получения необходимы все те же данные платежных карт. Звонки с подмененных номеров.

4. Звонки с подменных номеров

- Большинство банков имеют специальные номера, которые используются только для сообщений клиентам. Сбербанк, например, рассылает свои уведомления только с номеров 900 или 9000. Но существуют специальные программы-обманки, которые маскируют настоящий номер звонящего, и абонент видит знакомый ему идентификатор.

Проблема настолько обострилась, что 2.07.2021 Президент России подписал поправки в Федеральный закон «О связи»[2], позволяющие блокировать SMS-сообщения и голосовые звонки с подменных номеров. Операторы лишаются права менять истинный телефонный номер звонящего и обязаны подключиться к специальной службе Роскомнадзора. Частично закон вступает в силу 1.12.2021, а полностью — с 1.05.2022 года. Нет сомнений, что эта мера резко осложнит жизнь телефонным мошенникам.

5. Махинации со счетами мобильных телефонов

- Самый распространённый вариант такого мошенничества — сообщение или звонок об ошибочном переводе денег на счёт мобильного телефона и просьба вернуть их владельцу. Могут быть даже угрозы обращения в полицию или оператору с требованием блокировки телефона.

6. Сообщения о попавшем в беду родственнике и просьбы о помощи

- Панический звонок о попавшем в беду родственнике обычно случается среди ночи, полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счёт мобильника. Метод крайне жестокий, известны случаи инфарктов от подобных новостей.

7. Сообщения о выигрыше в лотерею

- Отличная новость сопровождается требованием перевода на покрытие технических издержек самой лотереи. Здесь расчёт на незнание законодательства РФ[3], согласно которому все расходы организаторов ложатся на них самих.

8. Сообщения-«грабители»

- Жертве приходит SMS с просьбой перезвонить по мобильному номеру, где ему сообщают якобы должны сообщить важную новость (о выигрыше в лотерею, проблемах с банковской картой, получении наследства). На звонок долго нет ответа, а после отключения обнаруживается, что со счёта списана большая сумма.

Мошенники используют возможность зарегистрировать сервис с платным звонком. Обычно подобные сервисы развлекательные и обязательно сообщают о платности в рекламе. Но мошенники этого не делают и за любой звонок по этому телефону взимают немалую плату.

9. Махинации с короткими номерами

- **Жертве приходит сообщение о том, что ей пришло сообщение в некий мессенджер, и его можно получить, пройдя по ссылке. После чего в смартфон внедряется вирус, получающий полный контроль над гаджетом.**

10. Телефонные вирусы

- Жертве приходит сообщение о том, что ей пришло сообщение в некий мессенджер, и его можно получить, пройдя по ссылке. После чего в смартфон внедряется вирус, получающий полный контроль над гаджетом.

Как противодействовать телефонным мошенникам

Может сложиться впечатление, что от телефонных мошенников нет спасения. Но службы безопасности банков активно им противодействуют. Сбербанк, например, разработал и внедрил систему кибербезопасности с использованием искусственного интеллекта. Все звонки, касающиеся переводов или снятия средств со счетов, контролируются и таким образом выявляются признаки преступной деятельности. В базе данных банка множество мошеннических колл-центров и 130 преступных схем. На

экране онлайн-банкинга появляется красный транспарант в случае подозрения о мошеннической операции. МВД РФ к концу 2021 года планируем запустить специальный сервис «Антимошенник» для борьбы с подобной преступной деятельностью. В интернете существует достаточно много сервисов для того, чтобы определить если не владельца конкретного телефонного номера, то по крайней мере город или страну, откуда пришел звонок. До 40% таких сообщений производятся из-за границы, еще 40% — из мест заключения. В любом случае поможет звонок в проверенную службу безопасности или колл-центр банка, а не по указанному грабителем номеру.

Можем порекомендовать конкретные методы защиты от телефонных мошенников.

1. Как вычислить телефонного мошенника?

- Чаще всего мошенники представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящий сообщает о попытке взлома или блокировки банковской карты, подозрительных действиях в интернет-банке, пропущенном платеже по кредиту или угрозе штрафа по надуманному обвинению. На самом деле

сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают другими способами.

2. Как вести себя во время разговора с незнакомым человеком?

- Получив звонок от незнакомого человека, обратите внимание на то, что и как он хочет вам сообщить.

Мошенники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. В такой ситуации важно сохранять спокойствие. Даже если вам угрожают потерей всех денег на счетах, не спешите выполнять требования звонящего.

Также мошенник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом

«да». Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить тему.

Если вам звонят из банка — попробуйте задать уточняющие вопросы, например, о состоянии счета или последних операциях по карте. Скорее всего, злоумышленник ничего не сможет ответить. Если вам предлагают какую-либо выплату — уточните основание, на котором она производится.

3. Какую информацию нельзя сообщать собеседнику по телефону?

- Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

4. Как составить заявление по факту мошенничества по телефону?

- Если вы столкнулись с телефонным мошенничеством — как можно скорее обратитесь в полицию, даже если вы не отправляли деньги или данные карты.

В заявлении подробно опишите обстоятельства происшествия — время звонка номер телефона, ФИО и «должность» звонящего, содержание и итог разговора, если вы переводили деньги — отправленную сумму. В качестве основания укажите статью 159 УК РФ (если

мошенник смог получить от вас деньги) и часть 3 статьи 30 УК РФ (если этого сделать не удалось). Если у вас есть запись звонка (его можно записать с помощью специального приложения) — приложите ее к заявлению.

Заявление будет рассматриваться в течение 10-30 дней. По итогам будет принято решение о возбуждении уголовного дела. Если вы получили отказ, то можно обжаловать его в прокуратуре — для этого потребуются копия заявления и постановление об отказе.

5. Какая ответственность предусмотрена за телефонное мошенничество?

- Телефонное мошенничество попадает под статью 159 Уголовного кодекса РФ[4]. В зависимости от тяжести и обстоятельств преступления за него могут быть предусмотрены штраф в размере до 500 000 рублей, принудительные, обязательные или исправительные работы, либо лишение свободы на срок до десяти лет со штрафом или без него.

6. Насколько реально получить компенсацию жертве мошенника?

- Привлечь телефонного мошенника к ответственности достаточно сложно. Опытные злоумышленники тщательно заметают следы — подменяют номера, регистрируют SIM-карты на чужие паспортные данные, используют ПО для сокрытия местоположения. Много мошенников работает из мест лишения свободы или других стран. Добраться до них

и привлечь к ответственности в таком случае становится еще сложнее.

Тем не менее, не стоит опускать руки и считать, что добиться справедливости нельзя. Каждое поданное заявление правоохранительные органы будут учитывать при последующих случаях мошенничества. Чем больше пострадавших обращаться в полицию, тем выше вероятность того, что злоумышленник будет найден и наказан.

1. Как обезопасить пожилых людей от телефонных мошенников?

В общем — будьте бдительны и не станете жертвами телефонных мошенников.

- -Никому не сообщайте код с обратной стороны карты, коды из SMS, данные для входа в интернет-банк;
- Для перевода денег используйте только официальные сервисы банков, платежных систем и торговых площадок;
- Не перезванивайте по незнакомым номерам, даже если вам поступил звонок, который был сразу же сброшен;
- Звоните в банки и государственные структуры только по их официальным номерам;

- Не переходите по подозрительным ссылкам, которые отправляют звонящие;

- Если вам позвонили якобы из банка и сообщили о блокировке или других проблемах с картой — сбросьте звонок и перезвоните в банк сами;

- Если вы потеряли карту или сообщили подозрительному человеку ее номер — сразу же заблокируйте ее и запросите перевыпуск.

https://soc-part.ru/

АССОЦИАЦИЯ
СОЦИАЛЬНОЕ
СОТРУДНИЧЕСТВО
Экология

191023, Россия, Санкт-Петербург,
Большой Казачий переулок, д11А
ИНН 7838087362, КПП 783801001
www.soc-part.ru
res-ecolog@mail.ru