Банк России

КИБЕРМОШЕННИЧЕСТВО: **ПРОТИВОДЕЙСТВИЕ НОВЫМ УГРОЗАМ**

КИБЕРМОШЕННИЧЕСТВО: КОЛИЧЕСТВО ОПЕРАЦИЙ И УЩЕРБ*

Банк России

9 месяцев 2025

ТЫС. ЕДИНИЦ

1 029,8

МЛРД РУБЛЕЙ

21,4

Предотвращено 111 млн мошеннических операций на 11,5 трлн рублей

	ТЫС. ЕДИНИЦ	МЛРД РУБЛЕЙ
2024	1 197,4	27,5
2023	1 165,9	15,8
2022	876,6	14,2
2021	1 035	13,6
2020	773,2	9,8

В 2024 году банки предотвратили 72,2 млн мошеннических операций на 13,5 трлн рублей

* Физические и юридические лица

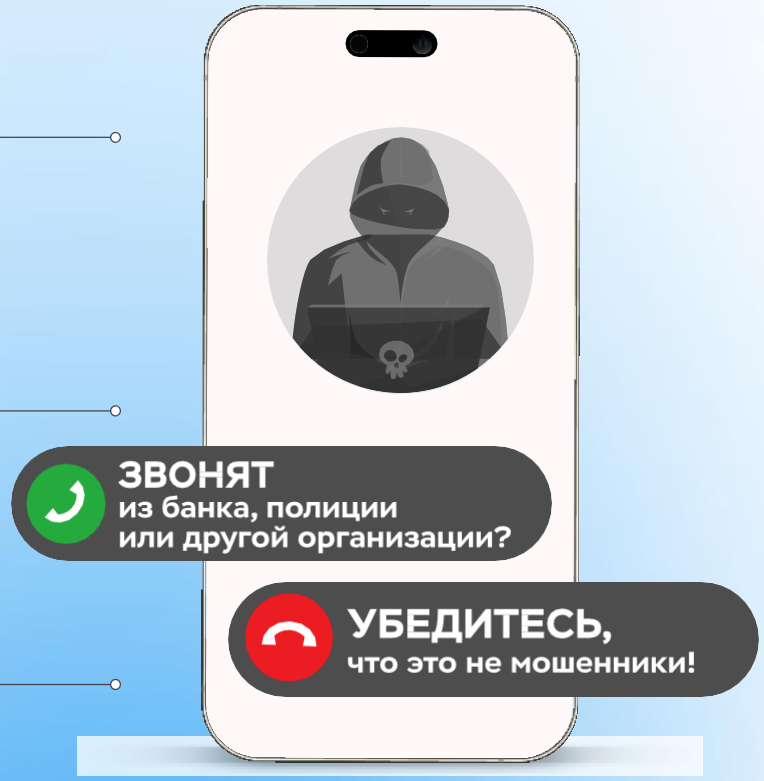
ТЕЛЕФОН – ОСНОВНОЙ ИНСТРУМЕНТ МОШЕННИКОВ

Банк России

Обман или злоупотребление доверием

Психологическое давление

Манипулирование



Под влиянием мошенников человек добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для хищения денег

ЛЖЕСОТРУДНИКИ ЦЕНТРОБАНКА: ФАЛЬШИВЫЕ ДОКУМЕНТЫ

Банк России

ПИСЬМО

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы стали жертвой мошеннических действий, а именно заключения договора на потребительский кредит, который был оформлен мошенническим путем. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого номера лицевого счета.

Ниже представлены Ваши действующие реквизиты:

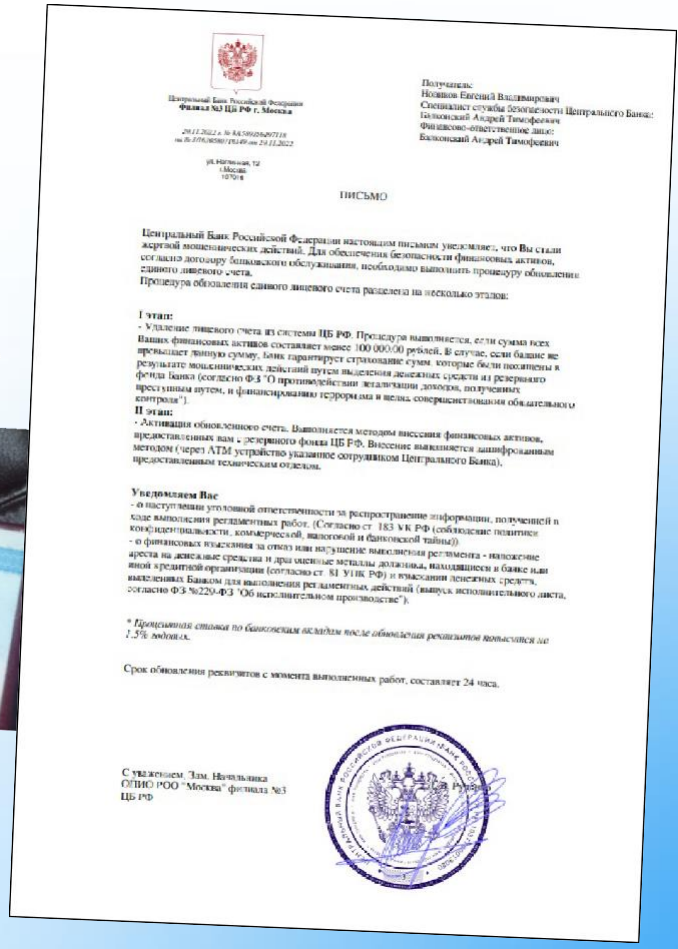
Обновленный счет: **40817810840148881854**

Срок действия обновленных реквизитов составляет 24 часа.

Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: Филиал №3 ЦБ РФ г. Москва
БИК: 044536002
ИНН: 7702235133
Корр.сч.: 30101810400000000138

С уважением, Зам. Начальника
ОПИО РОО "Москва" филиала №3
ЦБ РФ



ПИСЬМО

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого лицевого счета.
Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Удаление лицевого счета из системы ЦБ РФ. Процедура выполняется, если сумма всех Ваших финансовых активов составляет менее 300 000.00 рублей. В случае, если баланс не превышает данную сумму, Банк гарантирует страхование сумм, которые были похищены в результате мошеннических действий путем выделения денежных средств из резервного фонда Банка (согласно ФЗ "О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма и целях совершенствования обязательного контроля").

II этап:
- Активация обновленного счета. Выполняется методом внесения финансовых активов, предоставленных вам с резервного фонда ЦБ РФ. Внесение выполняется шифрованным методом (через АТМ устройство указанное сотрудником Центрального Банка), предоставленным техническим отделом.

Уведомляем Вас
- о наступлении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (Согласно ст. 183 УК РФ (обязующие политике конфиденциальности, коммерческой, налоговой и банковской тайны))
- о финансовых взысканиях за отказ или неуспешное выполнения регламента - наложение ареста на денежные средства и драгоценные металлы должника, находящиеся в банке или иной кредитной организации (согласно ст. 81 УПК РФ) и изъятии денежных средств, выделенных Банком для выполнения регламентных действий (выпуск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

** Процентная ставка по банковским вкладам после обновления реквизитов поднимается до 1,5% годовых.*

Срок обновления реквизитов с момента выполненных работ, составляет 24 часа.

С уважением, Зам. Начальника
ОПИО РОО "Москва" филиала №3
ЦБ РФ

ПРИЗНАКИ ФИШИНГОВЫХ САЙТОВ

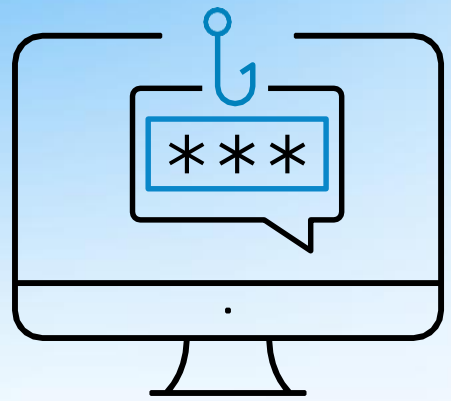
Банк России

- Ошибки в адресе сайта
- Сайт состоит из 1 страницы (только для ввода данных)
- В адресной строке отсутствует значок замка
- В названии сайта нет https://
- Ошибки в тексте и недочеты в дизайне
- Побуждение ввести свои личные/финансовые данные
- Предложение скачать файл, установить программу

Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания!

ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ В ИНТЕРНЕТЕ

Банк России



- Интернет-магазины и аукционы
- Онлайн-опросы и конкурсы
- Восстановление кредитной истории
- Сообщение о крупном выигрыше или выплате от государства
- Заманчивое предложение о работе
- Льготные кредиты
- Туристические путевки со скидкой
- Сбор «пожертвований» для детей, больных, животных и т. д.
- Предложение вложиться в высокодоходные инвестиции

Не верьте слепо предложениям в Интернете — проверяйте информацию на достоверность!

ПРИЗНАКИ ДИПФЕЙКА

Банк России

1. Неестественная, монотонная речь
2. Дефекты звука
3. Несвойственная мимика
4. Дефекты изображения

Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ ОТ КИБЕРМОШЕННИКОВ

Банк России

1. **Не сообщайте никому** личную и финансовую информацию (данные карты)
2. **Не читайте сообщения и письма** от неизвестных адресатов и **не перезванивайте** по неизвестным номерам
3. **Не переходите по сомнительным ссылкам** и **не скачивайте** неизвестные файлы или программы
4. **Установите на все свои гаджеты антивирусные программы** и регулярно обновляйте их
5. **Заведите отдельную банковскую карту** для покупок в Интернете

Будьте бдительны: не действуйте второпях и проверяйте информацию!
Расскажите об этих правилах поведения своим друзьям и знакомым

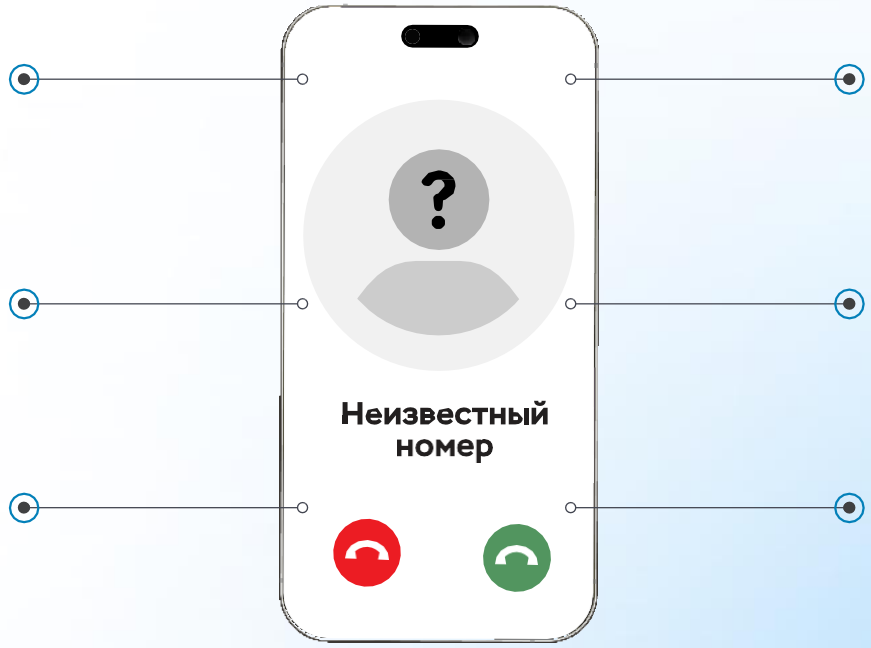
КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

Банк России

Не отвечайте на звонки с незнакомых номеров

Прервите разговор, если он касается финансовых вопросов

Не торопитесь принимать решение



Самостоятельно позвоните близкому человеку / в банк / в организацию

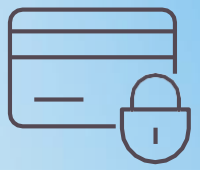
Проверьте информацию в Интернете или обратитесь за помощью к близким

Не перезванивайте по незнакомым номерам

Возьмите паузу и спросите совета у родных и друзей!

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ

Банк России



1 ЗАБЛОКИРУЙТЕ КАРТУ

- в мобильном приложении банка
- по телефону горячей линии банка
- лично обращением в отделение банка

СРАЗУ ЖЕ

2 СООБЩИТЕ В БАНК

- при личном обращении в отделение банка
- в мобильном приложении крупных банков

В ТЕЧЕНИЕ СУТОК

3 НАПИШИТЕ ЗАЯВЛЕНИЕ В ПОЛИЦИЮ

- при личном обращении в ближайший отдел ОВД

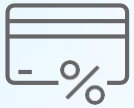
КАК МОЖНО СКОРЕЕ

ДРОППЕРЫ

Банк России

Дроппер (дроп) — это помощник злоумышленников, который с использованием своих карт или онлайн-банка помогает мошенникам выводить и обналичивать похищенные у людей деньги

Студенты



Люди с большим количеством кредитов

Уязвимые слои населения

Иногородние рабочие

Чем занимаются дропперы:

- **Получают** на свои счета деньги и передают их другим лицам — наличными или переводом
- **Принимают** наличные деньги, вносят их на свои счета для последующего перевода
- **Предоставляют** злоумышленникам банковские карты или доступ к онлайн-банку

ВОВЛЕЧЕНИЕ В ДРОППЕРСТВО

Банк России

ГДЕ И КАК ИЩУТ ДРОППЕРОВ

Основной канал — Интернет (социальные сети, мессенджеры, электронная почта)

- Обещают высокий доход и удаленный режим работы
- Не требуют опыта работы и специальных навыков
- Единственное требование — наличие банковских карт или доступа к онлайн-банку

ЧТО ГРОЗИТ ДРОППЕРАМ

- Дропперы попадают в базу данных Банка России
- Банки ограничивают им доступ к онлайн-банку и картам
- Для дропперов такая работа заканчивается уголовным наказанием

ДРОППЕРЫ: МЕРЫ ПРОТИВОДЕЙСТВИЯ

Банк России

1

Сейчас банки вправе блокировать дропперам карты и отключать доступ к онлайн-банку.
А при получении сведений о них от правоохранительных органов это делается обязательно

2

Человек, сведения о котором есть в базе данных Банка России, не может переводить себе или другим людям с помощью карт или онлайн-банка, а также снимать наличные через банкомат больше 100 тыс. рублей в месяц

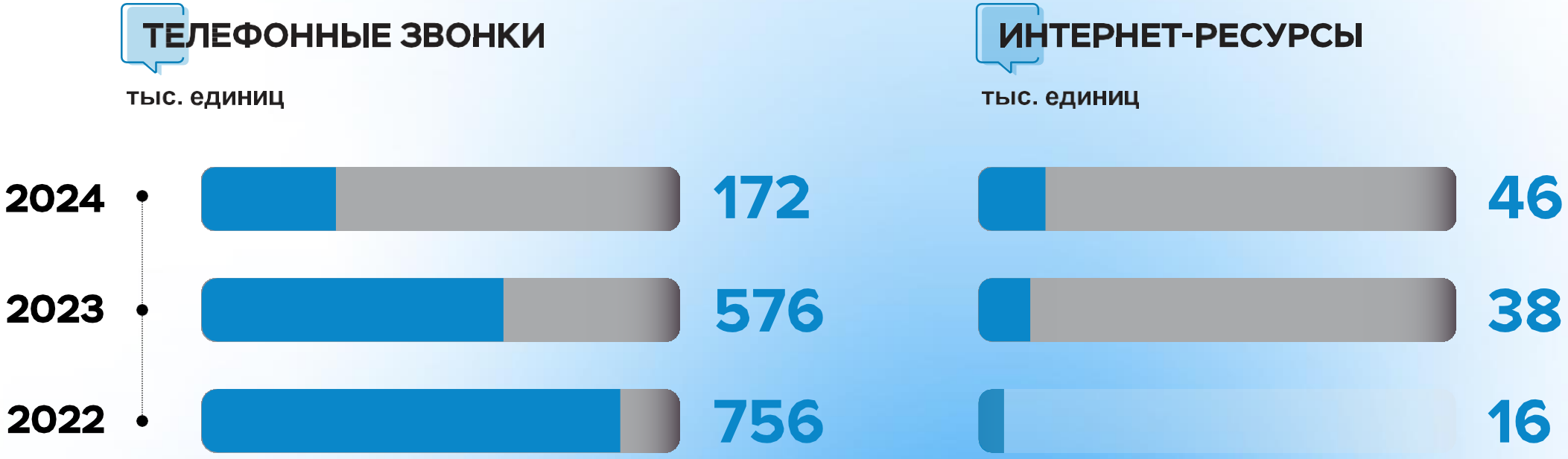
3

Банки не выдают новые карты дропперам, информация о которых есть в базе данных Банка России

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСКИМ ТЕЛЕФОННЫМ ЗВОНКАМ И ИНТЕРНЕТ-РЕСУРСАМ

Банк России

Банк России инициирует блокировку телефонных номеров и интернет-ресурсов, которые используют злоумышленники для обмана людей*



За 9 месяцев 2025 года Банк России инициировал блокировку 57,3 тыс. телефонных номеров, 28,4 тыс. интернет-ресурсов

* Сайты, страницы в соцсетях, приложения, телефонные номера

ПРИЗНАКИ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ ПРИ СНЯТИИ НАЛИЧНЫХ В БАНКОМАТАХ

Банк России

1 **Нехарактерное поведение клиента при снятии наличных через банкомат**

Например, непривычные время суток или местонахождение банкомата, нетипичные сумма или количество операций

2 **Превышение времени направления ответа карты на запрос банкомата**

3 **Нехарактерный способ снятия наличных**

Например, вместо пластиковой карты используется QR-код

4 **Направление запроса на выдачу наличных в течение 24 часов с момента:**

- предоставления кредита/займа, увеличения лимита на выдачу наличных или лимита по кредитной карте
- досрочного расторжения договора банковского вклада на сумму более 200 тыс. рублей
- перевода на свой счет по СБП со своего счета в другом банке более 200 тыс. рублей

5 **Информация об уровне риска осуществления мошеннической операции, полученная от АО «НСПК»**

ПРИЗНАКИ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ ПРИ СНЯТИИ НАЛИЧНЫХ В БАНКОМАТАХ

Банк России

6 **Нетипичная телефонная активность за 6 часов до направления запроса на снятие наличных (в том числе в мессенджерах)**

7 **Информация о пяти и более отказах в выдаче наличных в течение календарного дня**

Например, в связи с ошибками при вводе ПИН-кода, превышением лимита кредитования и т. д.

8 **Информация о нетипичных параметрах и характеристиках устройства клиента**

Например, наличие ВПО, нетипичный провайдер связи, активный VPN-сервис, смена номера в личном кабинете, нетипичная операционная система и т. д.

9 **Наличие сведений о клиенте или его электронных средствах платежа в государственной информационной системе «Антифрод»**

(критерий начнет применяться с 01.03.2026, когда заработает система)

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ ПРИ СНЯТИИ НАЛИЧНЫХ ЧЕРЕЗ БАНКОМАТЫ

Банк России

Банки, выпустившие платежную карту, обязаны перед выдачей наличных через банкоматы проводить проверку на наличие признаков совершения мошеннической операции

Если банк выявляет хотя бы один признак, вводится лимит на выдачу наличных через банкоматы на 48 часов на сумму не более 50 тыс. рублей в сутки с момента направления запроса на выдачу*

* Федеральный закон от 01.04.2025 № 41-ФЗ

ШЕСТЬ ПРИЗНАКОВ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ

Банк России

1. Реквизиты получателя денег есть в базе данных Банка России о мошеннических операциях
2. Нетипичная для клиента операция — например, по сумме перевода, периодичности, времени и месту совершения
3. Операция с устройства, которое ранее использовалось злоумышленниками и сведения о котором есть в базе данных регулятора
4. Сведения о получателе денег содержатся в собственной базе банка о подозрительных переводах
5. Есть информация о возбуждении уголовного дела по факту мошенничества в отношении получателя денег
6. Данные сторонних организаций о возможном мошенническом переводе (телефонная активность, рост числа входящих СМС-сообщений с новых номеров)

С 1 января 2026 года перечень признаков расширен до 12

Приказ Банка России № ОД-2506 от 5 ноября 2025 года

ЧТО ИЗМЕНИЛОСЬ С 25 ИЮЛЯ 2024 ГОДА*

Банк России

Двухдневный период охлаждения для переводов на мошеннические и подозрительные реквизиты из базы данных Банка России

Блокировка карты и онлайн-банка клиентов, которые занимаются выводом и обналичиванием похищенных денег

Возмещение похищенных денег в течение 30 календарных дней: если банк не приостановил мошеннический перевод или не уведомил об этом клиента, то он несет за это финансовую ответственность

* Внесены изменения в Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ

Банк России

1. **Банки и МФО обязаны проводить антифрод-мероприятия перед выдачей кредитов и займов**

2. **Если банк или МФО нарушат антимошеннические нормы и будет возбуждено уголовное дело по факту хищения заемных денег, то заемщик освобождается от исполнения обязательств до вступления в силу приговора суда по уголовному делу**

3. **Период охлаждения для потребительских кредитов и займов:**

4 часа
для сумм от **50** тыс. до **200** тыс. рублей

48 часов
для сумм свыше **200** тыс. рублей

Федеральный закон от 13.02.2025 № 9-ФЗ

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ

Банк России

Период охлаждения не применяется в случаях оформления:

1. кредитов и займов до 50 тыс. рублей
2. ипотечных и образовательных кредитов, автокредитов (при зачислении денег продавцу автомобиля – юридическому лицу)
3. кредитов, по которым заемщик не позднее чем за 2 дня до заключения договора назначил уполномоченное (доверенное) лицо для подтверждения заключения договора
4. покупки товаров (услуг) в кредит при личном присутствии потребителя в магазине (организации)
5. кредитов на рефинансирование ранее взятых обязательств, если это не приведет к увеличению их размера
6. кредитов, обязательства по которым принимают несколько созаемщиков или по которым у заемщика есть поручители

Федеральный закон от 13.02.2025 № 9-ФЗ

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ

Банк России

- МФО при дистанционном оформлении займа зачисляют деньги на счет, только если сведения о заемщике и получателе денег совпадают
- Банки не перечисляют заемные деньги на счет человека, сведения о котором содержатся в базе данных Банка России о мошеннических операциях, если заемщик указал его реквизиты в качестве третьего лица для получения денег
- МФО отказывают в выдаче займа, если сведения о заемщике содержатся в базе данных Банка России о мошеннических операциях
- Будет ускорен обмен информацией между БКИ и кредиторами: БКИ будут обязаны принимать информацию, направляемую банками и МФО, и передавать ее им в онлайн-режиме (с 01.07.2026)
- Банки и МФО будут обязаны получать информацию из БКИ, фиксировать факт ее получения, хранить и учитывать ее в своих антифрод-процедурах (с 31.12.2026)

Федеральный закон от 13.02.2025 № 9-ФЗ