Осторожно – поддельные купюры!

На территории России растет число преступлений, связанных с изготовлением и сбытом поддельных денежных знаков, государственных ценных бумаг и иностранной валюты. Фальшивомонетчики используют современную технику и технологии, обеспечивающие их массовый выпуск. Подобная преступная деятельность создает потенциальную угрозу денежному обращению, становится одним из факторов, дестабилизирующих финансовую систему.

В настоящее время в обороте находится большое количество поддельных банкнот Банка России номиналом 1000 и 5000 рублей и участились факты обнаружения поддельных банкнот Банка России номиналом 2000 рублей.

Основные признаки подлинности банкноты Банка России образца 2017 года номиналом 2000 рублей:

Какие фальшивые купюры бывают?

В теории принято различать следующие виды подделок бумажных денежных знаков:

- Полная фальсификация с помощью оригинальных способов. Этот вид подделки отличается высоким качеством. При изготовлении фальшивых купюр таким способом выбираются лучшие материалы. Как правило, преступники, являются «мастерами» своего дела и затрачивают много времени для изготовления купюры. В обиходе такие деньги практически не встречаются.
- Полная подделка по внешнему виду. В данном случае используются различные вспомогательные средства: краски, печати, волокна. В итоге купюра визуально отличается от подлинной по своим характеристикам и явно уступает качеству.
- Частичная фальсификация. Встречается часто, особенно при подделке долларов США. Преступники изменяют один номинал купюры на другой (на больший) путем дорисовки, допечатки нолей.

Для повышения качества фальшивых купюр злоумышленники используют различные методы и оборудование – принтеры и копировальную технику. Для придания деньгам использованного вида их загрязняют, мнут, тонируют. Поддельность таких купюр выдает бумага. Она более мягкая на ощупь и не отличается прочностью. Чтобы не стать жертвой фальшивомонетничества, следует знать критерии подлинности денежных средств.

Основные признаки настоящих банкнот:

- **Водяной знак – один из основных элементов.** Представляет собой изображение на бумаге, которое отчетливо видно на просвет. Его контуры плавные, имеют различные оттенки – от темных до светлых. Рисунки знаков отличаются друг от друга в зависимости от номинала. В фальшивых купюрах такие знаки либо отсутствуют, либо напечатаны однотонно (нет плавных переходов оттенков).
- Защитные волокна. Они короткие, разноцветные, хаотично расположенные в структуре бумаги. На поддельной банкноте волокна могут быть нарисованы, напечатаны, вклеены либо вовсе отсутствовать.

- Защитная нить. На просвет она сплошная. На оборотной стороне купюры невооруженным взглядом видны фрагменты нити, напоминающие по форме прямоугольники. В подделке нить отличается цветом, материалом изготовления. Она может быть вклеена либо дорисована.
- Если держать банкноту под углом, то на ней можно увидеть скрытое изображение.

В поддельных купюрах, изготовленных при помощи копировально-множительной техники или принтера, такие изображения отсутствуют.

- На лицевой стороне банкноты имеются тонкие параллельные линии. Они образуют поле, которое является монотонным. При рассмотрении купюр под острым углом, на нем появляются радужные (муаровые) полосы. Эффект достигается следующим образом: лучи, попадая на тиснения бумаги, отражаются под разным углом. В результате создается перелив цвета. Как правило, на поддельных банкнотах элемент отсутствует.
- Микроотверстия, которые образуют цифровое обозначение номинала. Бумага в указанном месте гладкая, в отличие от подделки, так как отверстия выполнены лазером.
- При изготовлении банкнот применяется цветопеременная краска. При наклоне купюры краска меняет цвет в определенных местах, так как содержит переменные пигменты. Изменения цвета видны визуально.
- Рельефные изображение и текст. Данные элементы предусмотрены для людей с ослабленным зрением, так как на ощупь можно легко различить подлинную купюру от подделки.
- Микротекст. Элемент состоит из букв и цифрового обозначения номинала. Можно распознать текст без лупы, так как он хорошо читаем.

Приведенные основные способы защиты банкнот позволяют любому человеку самостоятельно выявить признаки подделки. Но, следует помнить, что качественно изготовленные фальшивые деньги отличить от подлинных визуально очень тяжело, а порой невозможно. Это обусловлено тем, что преступники тщательно продумывают свои действия, а в технологию изготовления внедряют новые средства и методы.

Полицейские обращаются к гражданам: если вы обнаружили у себя поддельную денежную купюру, либо денежную купюру, вызвавшую сомнение в подлинности - необходимо сразу же обратиться в полицию с указанной поддельной купюрой или в любое банковское учреждение. Постараться вспомнить и пояснить сотрудникам полиции, откуда у него появилась данная купюра. При обнаружении поддельной купюры не пытаться сбыть ее, так как в данном случае гражданин автоматически становится субъектом преступления (сбытчиком) и будет привлечен к уголовной ответственности по ст. 186 УК РФ (предусмотрено наказание в виде лишения свободы на срок до 15 лет).

Виды мошенничества с банковскими картами

Мошенничеством в сети уже никого не удивишь, но сегодня все большую популярность набирает обман с использованием личных банковских карт граждан. Мошенничество с банковскими картами проходит настолько мастерски, что обманутые даже не сразу понимают о незаконном списании денежных средств со счета.

Как правило, в большинстве случаев владельцы карт самостоятельно отдают деньги, поэтому не прибегают к способам их возврата. Далее будет подробно рассмотрены подобные ситуации, а также приведены случаи, когда обманутые смогут вернуть денежные средства обратно.

Виды и как все происходит

Чтобы понять, что такое мошенничество с использованием банковских карт, необходимо рассмотреть возможные его виды.

Новые способы и схемы мошенничества

Схем мошенничества очень много, большинство из них уже четко отработаны. Но сегодня можно выделить еще один способ «законного» списания денежных средств с банковской карты – это звонок сотрудников банка.

Разумеется, звонят мошенники, но со знакомых единых номеров, которые в точности неизвестны клиентам финансового учреждения. Опытные преступники могут позвонить с единого утвержденного номера банка, но пропасть сразу после перечисления денег.

Приведенная схема мошенничества проста:

- На номер потерпевшего приходит сообщение с единого номера 900, в котором говорится о том, что кто-то из знакомых запросил денежные средства путем перечисления ему на карту. Тут же приписывается, что перечисление проводится с разрешения получателя сообщения путем отправки в ответ кода или автоматически через 600 секунд. Получается, что выхода у получателя сообщения нет – это и приводит к панике.
- Далее на номер поступает звонок от сотрудника банка, который вежливо сообщает о начавшемся мошенничестве и предлагает помощь в его предотвращении.
- Для этого клиенту банка следует оставаться на линии и отправить сообщение с кодом, присланным в письме. К коду может быть приложена еще одна комбинация цифр, продиктованная сотрудником банка. Также в сообщении необходимо написать «отмена перевода».
- После отправленного сообщения деньги с карты снимаются, звонок отключается, и сотрудник банка исчезает.

Дальнейшие попытки связаться с банком заканчиваются успехом, но найти того злополучного сотрудника уже не представляется возможным.

При детализации звонков на мобильный телефон можно обнаружить единый мобильный номер банка, поступивший на сотовый обманутого, но из банка этот звонок не поступал – в их распечатке телефонных звонков номера потерпевшего нет.

Через смс по мобильному телефону

Самый распространенный способ мошенничества – это через сообщение по мобильному номеру.

На номер пострадавшего приходит сообщение о блокировке карточки. Для разблокирования необходимо сделать обратный звонок на короткий номер.

Обманутый звонит мошеннику, который представляется сотрудником банка и говорит о необходимости назвать все данные – номер карты, кодовое слово и пин-код карточки. Это «требуется» для совершения операции по разблокировке.

Далее мошенник говорит о разрешении вопроса, но уже через несколько минут с карточки будут сняты все денежные средства. Владелец сам сообщил все данные, с помощью которых преступники сняли деньги.

Через мобильный банк

Через мобильный банк мошенничество определяется путем практики фишинга.

Схема проста:

- Владелец закачивает на свой смартфон приложение банка, которое помогает осуществлять операции с карточки, требуя обязательной ее привязки.
- Далее путем постоянных вирусных атак приложение заражается вирусом. В результате при включении приложения загружается фальшивое окно, требующее ввести данные карточки.
- Пользователь вводит данные, не подозревая, что автоматически позволяет снять со своей карточки деньги вирусной программе.

Аналогичным образом из интернета скачиваются приложения-вирусы, которые внешне схожи с оригиналами, но являются мошеннической системой. Пользователь привязывает карту и автоматически переводит денежные средства преступникам.

По номеру карты

Место совершения преступления зачастую может быть обнародовано самим владельцем банковской карты.

К примеру, он рассчитывается банковской картой в ресторане или кафе, где зачастую карту просто забирает официант и приносит уже после проведения оплаты. В это время данные карты можно списать или запомнить.

Даже в супермаркетах или автозаправках присутствует скрытая камера, которая позволяет быстро сфотографировать данные карточки. Далее происходит оплата некоторых товаров путем ввода ее номера.

С бесконтактными картами

Преступники скрываются в толпе, где на присутствие в руках какого-либо предмета не обратят внимания. Путем подобного бесконтактного «щелчка» можно снять с карты до 1 тыс. рублей без подтверждения операции кодом.

Через банкомат

Банкоматы – это настоящие системы мошенничества, которые дают волю преступникам придумывать все новые и новые схемы.

На данный момент можно выделить 3 основных метода:

- **Подставной банкомат.** В данном случае мошенники просто устанавливают свои аппараты, внешне схожи с настоящими банковскими системами. В результате устройство копирует всю информацию с карты и при пополнении денежными средствами снимает их.
- **Скимминг.** Мошенники предпочитают не устанавливать ложные банкоматы, а модернизируют уже установленные. В устройства устанавливаются фальш-накладки для считывания пин-кода, а также специальные считывающие дополнения для распознания магнитной ленты с последующим определением данных. В результате пользования банкоматом владелец карты сдает всю информацию о карте, после чего мошенники делают дубликат и снимают деньги при каждом поступлении.

- **Ввод вируса в банкомат.** Здесь не требуется банковская карточка. Мошенники, вводя вирус с устройство, могут с легкостью снимать денежные средства путем введения только кода, который заранее предусмотрен вирусной программой.

Это только основные способы снятия денежных средств с банковской карты путем применения банкомата.

В интернет-магазине

Мошенничество с применением банковской карты не обошло и интернет-магазины.

Здесь есть 2 схемы:

- Покупатель переводит денежные средства с карты для оплаты какого-либо товара, а он в итоге не приходит получателю. Это может быть дубликат сайта официального интернет-магазина, или вовсе сторонний сервис, предлагающий доставку товара известного магазина или гипермаркета продуктов.
- Второй способ более сложный и подразумевает последующее снятие денежных средств. Во-первых, владелец карты для приобретения определенного товара может наткнуться на вирусный фальшивый сервис, который попросту снимет деньги с введенного номера карты. Во-вторых, сайт запрашивает номер карты, с которой будет проводиться оплата, а далее пин-код, который требуется для подтверждения оплаты. Если пин-код будет введен, пройдет оплата, после чего покупатель будет ожидать своего товара. Разумеется, он не придет, а владелец потеряет драгоценное время на поиски преступников. В большинстве случаев он понимает об обмане только при последующем снятии денежных средств.

Аферы при переводе денег через Интернет

О подобном методе было уже сказано. Основным моментом здесь выступает запрос мошенников у владельца прислать или ввести в поле заявки пин-код карточки, чего делать категорически запрещается.

Доступной взору интернета на законодательном уровне становится следующая информация:

- номер карты;
- держатель карты – имя и фамилия;
- сроки действия карты;
- CVV или CVC2 карты – три цифры, которые указываются на обратной стороне пластика.

Вся остальная информация – пин-код, личные данные держателя карты, кодовое слово и прочее – должны оставаться только в познании самого владельца банковской карты.

На Авито

На Авито также практикуется несколько схем мошенничества:

- **Предоплата товара.** Никакой предоплаты товара без его личного осмотра быть не может, и администраторы сайта за этим тщательно следят.
- **Оплата товара через интернет с обязательным сообщением пин-кода.** Этого тоже быть не должно – оплату покупатель может провести самостоятельно в своем интернет-банкинге. Аналогично мошенники снимают денежные средства с карты продавца товара, представляясь покупателями. Здесь преступники просят продиктовать им номер карты, на которую можно перевести деньги, а затем просят сказать им код, пришедшей в смс-сообщении.

Никаких кодов при переводе денег получатель не должен получать – ему лишь придет сообщение о зачислении на счет.

- **Ввод данных в вирусную программу.** Происходит аналогичным способам, описанным ранее – покупатель вводит данные карты для оплаты товара, а программа определяет недостающее и просто снимает деньги в полном объеме.

К оплате товара через Интернет следует относиться с особенной осторожностью. Если вдруг запрашиваются коды, которые не должны быть получены владельцем карты, необходимо сообщить в Сбербанк или другое финансовое учреждение о совершающемся мошенническом преступлении.

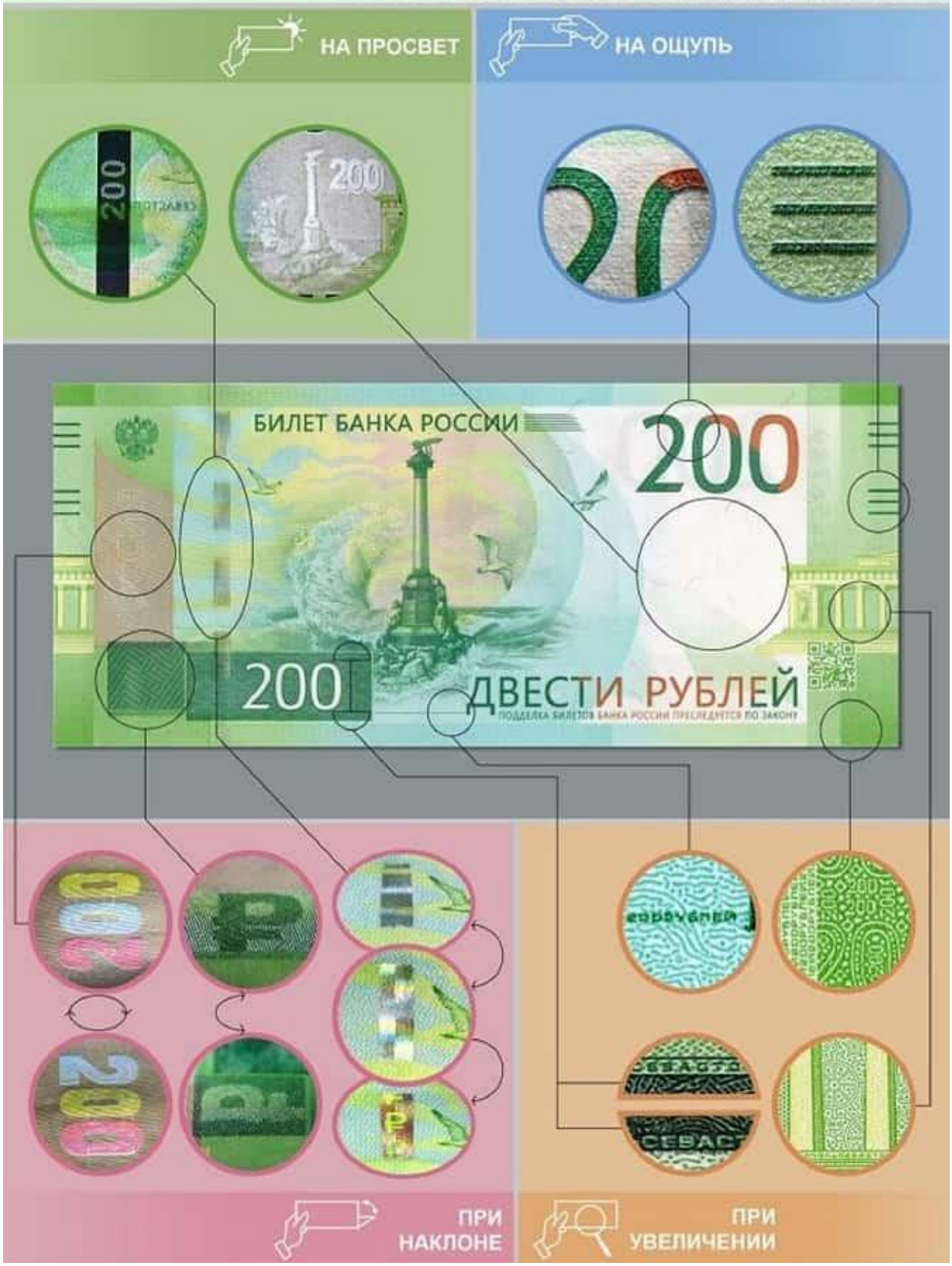
Нарушают ли закон легкий платеж МТС и автоплатеж Теле2?

Легкий платеж или автоплатеж подразумевают быстрый перевод денежных средств с банковской карты на счет мобильного телефона. Для подключения услуги приходится вводить номер карты и прочие данные карточки.

Но мошенники и здесь преуспели. Они звонят пользователю, у которого подключена услуга, и говорят о выдуманной ошибке, представляясь при этом оператором МТС или Теле2.

Чтобы исправить ситуацию, необходимо продиктовать код, который придет на номер пользователя смс-сообщением. Этот код присылается системой уже во время снятия денежных средств с карты – через несколько минут после заверения сотрудником об справленном положении со счета списываются деньги.

200 РУБЛЕЙ ОБРАЗЦА 2017 ГОДА

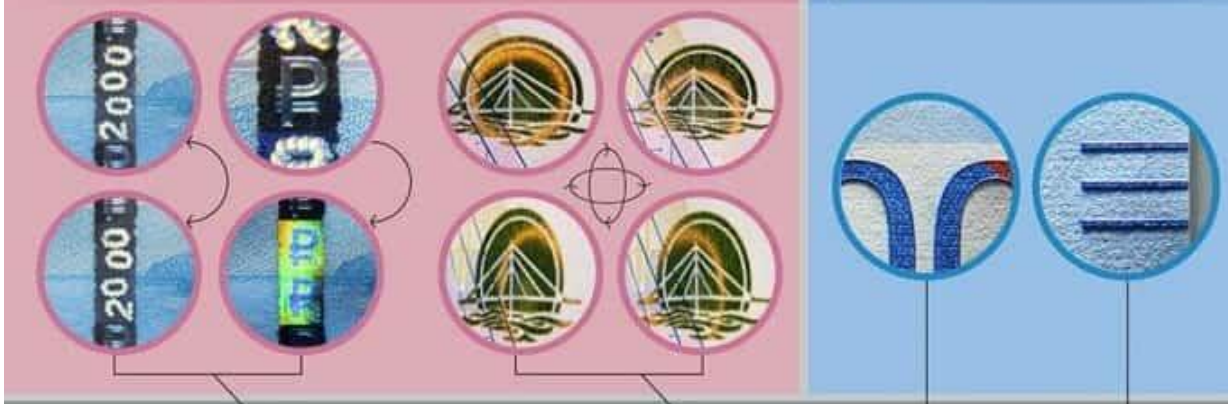


Как распознать фальшивку:

2000 РУБЛЕЙ ОБРАЗЦА 2017 ГОДА

ПРИ НАКЛОНЕ

НА ОЩУПЬ



ПРИ НАКЛОНЕ

НА ПРОСВЕТ

ПРИ УВЕЛИЧЕНИИ