# Как работает обработка платежей

Обработка онлайн-платежей проходит через ряд цифровых шлюзов. Если транзакция соответствует требованиям каждого отдельного платежного шлюза, она переходит к следующему. Последний шлюз – это банк продавца, куда зачисляются деньги.

Платежные шлюзы используются, чтобы безопасно передавать данные клиентов в процессе обработки платежей.

Структуру процесса оплаты на сайте с использованием сервиса Платформы состоит из следующих шагов:

**1. Клиент покупает онлайн на сайте**

Любой может попытаться купить что угодно в интернете. Но нет гарантии, что операция будет одобрена.

Когда Клиент оформил на сайте заказ на определенную сумму, выбирал способ оплаты «банковской картой» и нажал кнопку «оплатить», сайт получает от Платформы ссылку на платежную форму и перебрасывает Клиента на страницу платежного шлюза.

После того, как Клиент ввел данные по карте информацию обрабатывает платежный процессор.

**2. Платежный шлюз шифрует информацию о переводе**

Соединение с платежным шлюзом и передача информации осуществляется в защищенном режиме с использованием протокола шифрования SSL. В случае если Ваш банк-эмитент Клиента поддерживает технологию безопасного проведения интернет-платежей Verified By Visa или MasterCard SecureCode для проведения платежа также может потребоваться ввод специального пароля.

Наши технологии поддерживают 256-битное шифрование, что исключает кражу данных. Платежный шлюз кодирует платежные данные заказчика, чтобы они не попали в руки мошенникам.

**3. Процессинговый центр проверяет детали перевода**

После того, как платежный шлюз зашифрует все данные клиента, он передаст информацию в Процессинговый центр, который в свою очередь через информационные системы платежных систем направляет запрос в банк-эмитент карты Клиента, чтобы проверить состояние карт-счета клиента и возможность проведения транзакции.

### 4. Банк-эмитент принимает решение о переводе

Банк, выпустивший карту, подтверждает возможность сделки. Как только обработчик платежей передает запрос на перевод средств, банк решает, следует ли авторизовать транзакцию.

Обычно, если на платежном шлюзе или процессоре платежей нет «красных флажков», авторизация проходит быстро.

Однако, если что-то кажется подозрительным – например, тот факт, что покупатель обычно не тратит больше определенной суммы или оплата совершается из другой страны, – Процессинговый центр или Банк-эмитент могут заблокировать транзакцию.

Обычно транзакции отклоняются по следующим причинам:

- Недостаточно средств на счету
- Статус замороженного аккаунта
- Неверно указан номер кредитки или срок действия
- Лимиты переводов
- Карта была потеряна или украдена
- Адрес не соответствует
- Недопустимая проверка кода карты (CCV, CVV)

### 5. Перевод средств от Клиента к Продавцу

После того, как Процессинговый центр и Банк-эмитент одобряют сделку, в платежную систему через платежный шлюз передается информация, что деньги нужно доставить продавцу.

Платежная система, как связующее звено, запрашивает перевод денег из банка клиента в банк продавца. Поскольку транзакция уже одобрена, перевод выполняется, и поставщик получает платеж.

### 6. Продавец получает деньги

После успешной оплаты и списания средств с карт-счета клиента информация о результатах оплаты через указанную выше цепочку направляется на сайт магазина для завершения оформления продажи товара или услуги. Если же операция по каким-либо причинам невозможно, то магазин и клиент получает информацию об отказе.

# Безопасность платежей

Услуга перевода денег через процессинговые центры достаточно безопасна. Это достигается несколькими способами.

## 3D Secure

Метод дополнительной защиты платежей, установленный Visa, Mastercard и другими международными платежными системами.

3D Secure работает следующим образом: клиент оформляет заказ и нажимает “Оплатить”. Перед тем, как транзакция будет одобрена и с покупателя спишутся деньги, владельцу карты нужно подтвердить транзакцию. Например, через мобильное приложение банка или с помощью одноразового пароля, который приходит в sms.

Это снижает риск мошенничества и помогает убедиться, что картой пользуется действительно ее владелец.

## Служба проверки адресов (AVS)

AVS — это система для проверки платежного адреса держателя карты. Способ заключается в проверке достоверности информации, которая была предоставлена банку-эмитенту. AVS снижает риск мошенничества. Поддерживается Visa, MasterCard, Discover и American Express.

## Чарджбэк

Это еще один способ борьбы с мошенниками в интернете. Он помогает вернуть деньги, если мошенническая транзакция все-таки произошла. Например, клиент купил товар, а продавец ему ничего не прислал или прислал продукт плохого качества и не хочет менять.

Правда в этом случае клиенту придется доказать, что у него есть основания для чарджбека — подтвердить сам факт покупки и предоставить доказательства, что продавец неправ. Например, что он нарушил закон, правила платежных систем или условия пользовательского соглашения.

## Шифрование

Процесс, в котором кодируется личная информация клиента и транзакции для безопасной передачи данных в процессе обработки

платежа. Шифрование также является важной частью соответствия PCI DSS.

## PCI DSS

Международный стандарт безопасности платежных карт.

Это правила, которым должны следовать продавцы для предотвращения мошенничеств с кредитными картами. Если продавец принимает онлайн-платежи через провайдера услуг, то о PCI DSS можно не беспокоится. В этом случае проходить сертификацию по стандарту PCI DSS должен не продавец, а компания-провайдер. Она же и гарантирует безопасность и защиту платежных данных покупателей.