**3DSecure**

**Памятка клиента**

###

### Краткое описание технологии 3DSecure

3DSecure – это защищенный протокол авторизации пользователей. Технология разработана международными платежными системами для безопасной оплаты товаров и услуг по международным картам VISA и MasterCard в Интернете. Как это работает:

* + На первом шаге запрашиваются данные: номер карты, срок ее действия, имя держателя карты и код проверки ее подлинности (цифровой код на обратной стороне карты CVV2 или CVC2[[1]](#footnote-1)).
	+ На втором шаге используется протокол 3DSecure. Сайт магазина делает переадресацию на страницу банка-эмитента карты и предлагается ввести одноразовый код подтверждения[[2]](#footnote-2). Одноразовый код подтверждения можно получить из SMS-сообщения на своем мобильном телефоне, который был указан в заявлении на выпуск карты.
	+ Вся передаваемая информация от покупателя сохраняется на платежном сервере банка-эмитента, и интернет-магазин не имеет к ней доступа. Это защищает данные от хищения.

### Как узнать, что интернет-магазин поддерживает технологию 3DSecure?

Технологию безопасных платежей поддерживают более 300 000 интернет-магазинов и онлайн-сервисов по всему миру. Онлайн магазины, которые принимают платежи строго с использованием 3DSecure, можно узнать по размещенным на сайте логотипам:



### Как подключить банковскую карту к технологии 3DSecure?

В АО Банк «Национальный стандарт» технология 3DSecure доступна на всех картах VISA и MasterCard, эмитируемых банком и подключенных к услуге банка «SMS-оповещение»3

**Как оплачивать товары и услуги в Интернете картой, подключенной к 3DSecure?**

1. Убедитесь, что интернет-магазин или онлайн-сервис поддерживает технологию 3DSecure. Помните, что если указанная технология на сайте не поддерживается, то риск компрометации данных Вашей карты значительно выше.
2. Заказывая товар или услугу в Интернете, выберите способ оплаты банковской картой.
3. Укажите на сайте данные, которые запрашиваются:
	* номер карты (16 цифр на лицевой стороне карты),
	* CVV2 (три цифры на оборотной стороне карты, на полосе для подписи),
	* фамилию и имя (латинскими буквами, указаны на лицевой стороне карты),
	* срок действия карты (месяц и год, будьте внимательны - не перепутайте местами эти два поля),
	* другие сведения, которые запрашивает интернет-магазин (например, название банка, БИН - первые четыре или первые шесть цифр из номера карты и т.п.)
4. После этого Вы будете переадресованы на страницу ввода одноразового кода подтверждения, который вы получите посредством SMS.
5. После ввода одноразового кода подтверждения Банк осуществляет проверку данных. Если Банк подтверждает, что именно Вы являетесь держателем карты, а также наличие денег на счете, то покупка совершается.
6. Затем Вы вновь вернетесь на сайт интернет-магазина, а также получите SMS-сообщение с результатом (успешным или нет) совершения покупки.

3 **Услуга «SMS-оповещение»**, предоставляется в рамках услуги обслуживания счетов с использованием системы дистанционного банковского обслуживания, с использованием банковской карты и (или) её реквизитов. Данный сервис предназначен для повышения качества обслуживания Ваших банковских счетов и безопасности проведения операций с использованием систем дистанционного банковского обслуживания, а также банковских карт. **SMS-оповещение** – это возможность контролировать состояние счета с помощью мобильного телефона.

1. **CVV2/CVC2 - (англ. Card Verification Value 2)** – трёхзначный или четырёхзначный цифровой код на обратной стороне карты (в конце панели образца подписи), который используется Клиентом конфиденциально как способ удостоверения распоряжений по операциям с реквизитами карты в сети Интернет. [↑](#footnote-ref-1)
2. Уникальный набор символов, предоставляемый Клиенту на номер мобильного телефона. Позволяет подтвердить составление распоряжения уполномоченным на это лицом. [↑](#footnote-ref-2)