
Рекомендации для интернет-магазинов по увеличению оборотов и минимизации рисков, возможных в электронной коммерции

Цель : увеличить оборот интернет-магазина, обеспечить информацией об основных рисках и рекомендациями при работе с платежами по банковским карточкам

- Банк-эмитент – банк владельца карточки, выпустивший карточку;
- Банк-эквайер – банк интернет-магазина, с которым интернет-магазин заключил договор на интернет-эквайринг, АО «Народный Банк Казахстана»;
- Авторизационный запрос – запрос на одобрение транзакции банком-эквайером банку-эмитенту;
- Финансовая транзакция – транзакция списания средств с карт-счета покупателя, инициируется менеджером интернет-магазина.

- Chargeback – это возврат денежных средств владельцу карточки по требованию банка-эмитента.
- Если держателем карточки было предъявлено доказательство, позволяющее считать транзакцию недействительной, то средства должны быть возвращены держателю карточки.*

*** Но технология защиты 3-D Secure, предлагаемая Processing.kz, защищает вас от мошеннических chargeback-ов.**

Возможные риски, связанные с chargeback:

- Убытки (стоимость товара/услуги, расходы на доставку);
- Уровень chargeback
 - Согласно договору с Банком, в случае если уровень chargeback превысит 3% от суммы всех транзакций за 1 год, то Банк вправе приостановить обработку транзакций;
 - При превышении уровня chargeback 2% (Visa) и 1% (MasterCard) интернет-магазин заносится в глобальную программу мониторинга платежных систем.

Chargeback: виды и рекомендации

Недобросовестная работа интернет-магазина

Виды:

- Недоставка товара/услуги,
- Качество не соответствует заявленному.

Рекомендация:

- Внедрить четкую политику по обслуживанию покупателей и возврату товара.

Мошенничество

Виды:

- Операция совершена без участия владельца карточки,
- Данные карточки или сама карточка украдены.

Рекомендация:

- Использовать 3-D Secure,
- Осуществлять мониторинг транзакций.

Как предотвратить chargeback из-за мошенничества?

- Processing.kz использует и предлагает для всех своих клиентов систему защиты от мошенничества – 3-D Secure (см. далее).
- Ежедневно предоставляются данные для мониторинга транзакций:
 - Страна банка, выпустившего карту,
 - Результат проверки покупателя на 3-D Secure,
 - IP адрес, с которого совершается покупка,
 - Маскированный номер карточки покупателя.

3-D Secure – ваша защита от мошенничества

- 3-D Secure – это технология в основе глобальных программ Verified by Visa и MasterCard SecureCode, которая сводит риск мошенничества к нулю путем аутентификации по паролю, известному только настоящему владельцу карточки.
- Таким образом, покупателю недостаточно карточки, он дополнительно должен знать пароль.



* При участии владельца карточки в программе 3-D Secure

3-D Secure – ваша защита от ответственности

- Основная ценность 3-D Secure для интернет-магазина заключается в перераспределении ответственности за мошеннические транзакции – ответственность несет банк-эмитент или сам владелец карточки.
- 3-D Secure защищает от chargeback, связанных с мошенничеством, но не покрывает случаи некомпетентности интернет-магазина, недоставки товара/услуги.
- **Processing.kz и Народный банк участвуют в программе 3-D Secure!**

3-D Secure – ваша защита от ОТВЕТСТВЕННОСТИ

Processing.kz и Народный банк участвуют в программе 3-D Secure!

№	Банк-эквайер	Магазин	Банк-эмитент	Владелец карты	Ответственность
1	Есть 3D	Есть 3D	Есть 3D	Есть 3D	На владельце карты (секретный пароль)
2	Есть 3D	Есть 3D	Есть 3D	Нет 3D	На владельце карты (не воспользовался)
3	Есть 3D	Есть 3D	Нет 3D	Нет 3D	На банке-эмитенте или владельце карты (согласно договору)
4	Есть 3D	Нет 3D	Нет 3D	Нет 3D	На магазине (не воспользовался)
5*	Нет 3D	Нет 3D	Есть 3D	Есть 3D	На банке-эквайере или магазине (согласно договору)
6*	Нет 3D	Нет 3D	Есть 3D	Нет 3D	На банке-эквайере или магазине (согласно договору)
7*	Нет 3D	Нет 3D	Нет 3D	Нет 3D	Стандартная процедура разбирательства

* Не актуальны, так как Народный банк и Processing.kz имеют 3-D Secure.

- Помимо 3-D Secure защиты, менеджер интернет-магазина должен осуществлять мониторинг транзакций на основании своих данных о покупке, а также данных из отчетов Processing.kz;
- Вовремя выявить подозрительную транзакцию на одной из стадий проверок:
 - Авторизация
 - Списывание средств
 - Отправка товара/предоставление услуги
- Если транзакция подозрительная, принять решение об отказе в обработке заказа.

Мониторинг и решение об отказе

Одобренная авторизация

При подозрении на этапе авторизации - **провести дополнительную аутентификацию, отказать на основании имеющейся информации, и остановить отправку товара;**

Финансовое списание

После финансового списания средств и до отправки товара - **приостановить отправку товара и провести дополнительную аутентификацию;**

До доставки товара

По получению дополнительной информации (напр. о количестве покупок одним покупателем) – **приостановить отправку товара и провести дополнительную аутентификацию;**

Processing.kz предоставляет следующие данные для выявления подозрительной транзакции:

Данные от Processing.kz	На что обратить внимание	Действия
Страна банка эмитента	Страна с высоким риском мошенничества (см. далее)	Дополнительная аутентификация/решение об отказе
Результат проверки на 3-D Secure	Вводил ли покупатель код 3-D Secure пароль.	Если вводил, то риск минимален. Если не вводил, проверить на остальные параметры
IP адрес	Совпадает ли IP адрес и адрес доставки. Не используется ли анонимный proxy-сервер	Дополнительная аутентификация/решение об отказе
Маскированный номер карточки	Используются для дополнительной аутентификации (см. далее)	

Общепринятый список стран с высоким риском мошенничества

Ангола

Египет

Гана

Кот-д'Ивуар

Литва

Таиланд

Малайзия

Сингапур

Испания

Австралия

Индонезия

Бразилия

Нигер

Нигерия

Гонконг

Тайвань

Филиппины

Болгария

Великобритания

Украина

Намибия

Румыния

Аргентина

Чили

Албания

Перу

Узбекистан

Республика Конго

Мозамбик

Танзания

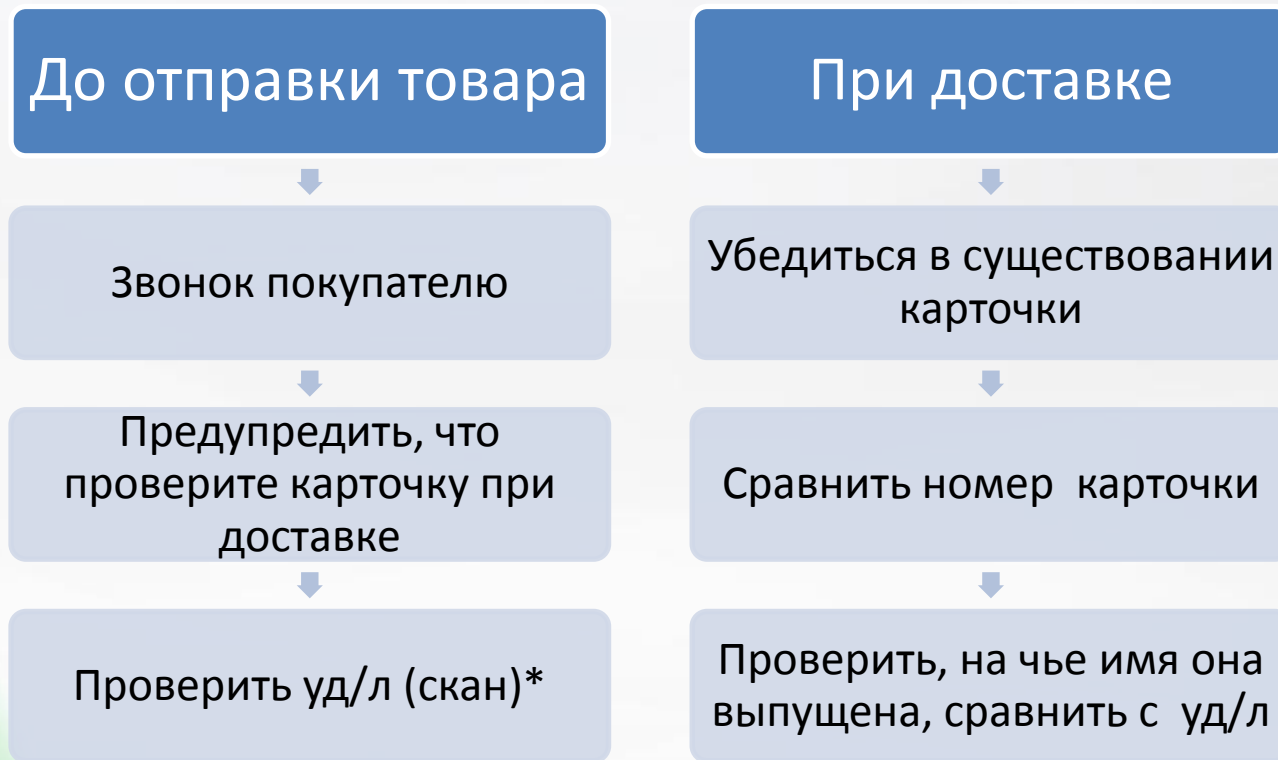
Мониторинг – признаки подозрительной транзакции

Также интернет-магазин может использовать свои данные о заказе для выявления подозрительной транзакции:

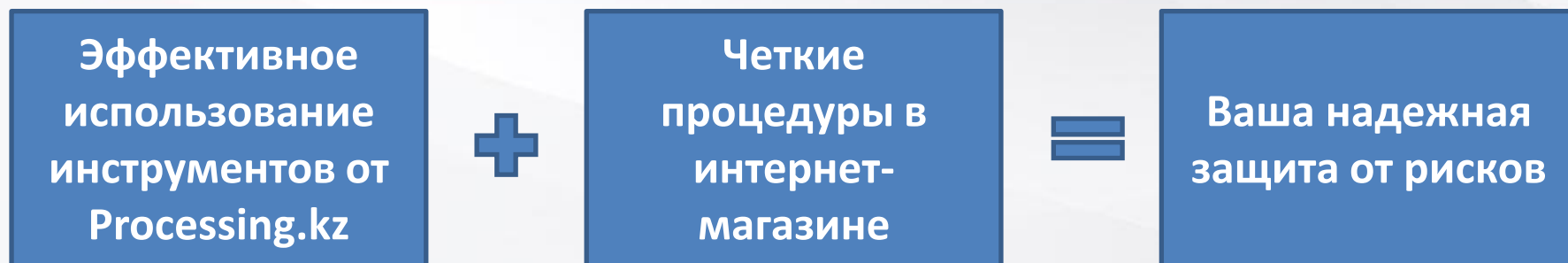
Данные	На что обратить внимание	Действия
1) Время совершения покупки	1) Покупка совершается на крупные суммы в ночное время, либо несколько покупок совершается с небольшим промежутком времени	1) Дополнительная аутентификация/решение об отказе
2) Характеристики покупателя и покупок	2) Новый посетитель сайта делает покупку на большую сумму относительно средней покупки в вашем интернет-магазине	2) Дополнительная аутентификация/решение об отказе

Дополнительная аутентификация покупателя

При подозрении на мошенничество, до отправки товара и проведения финансовой транзакции убедитесь, что покупатель является владельцем карточки:



* При ситуации, когда заведомо известно, что покупатель и получатель товара разные лица, рекомендуется использовать имеющиеся у интернет-магазина стандартные методы проверки.



- Processing.kz предлагает для вас защиту от мошенничества 3-D Secure и данные для мониторинга и выявления подозрительных транзакций;
- Решение об одобрении покупки, отправке товара и списании средств принимается интернет-магазином на основании собственных данных и дополнительных предоставленных Processing.kz.

- Интернет-магазин – это перспективный, выгодный канал продаж с неограниченными возможностями в рекламе и привлечении новых клиентов;
- Компания Processing.kz всегда готова сотрудничать с вами, изучать ваши нужды и пожелания ваших клиентов, разрабатывать специальные программы и работать над успехом вашего интернет-магазина.

СПАСИБО ЗА ВНИМАНИЕ!

Адрес офиса:

050022 г. Алматы

ул. Шевченко, 118, оф. 116

Тел.: +7 727 244 04 77

Web-сайт: www.processing.kz