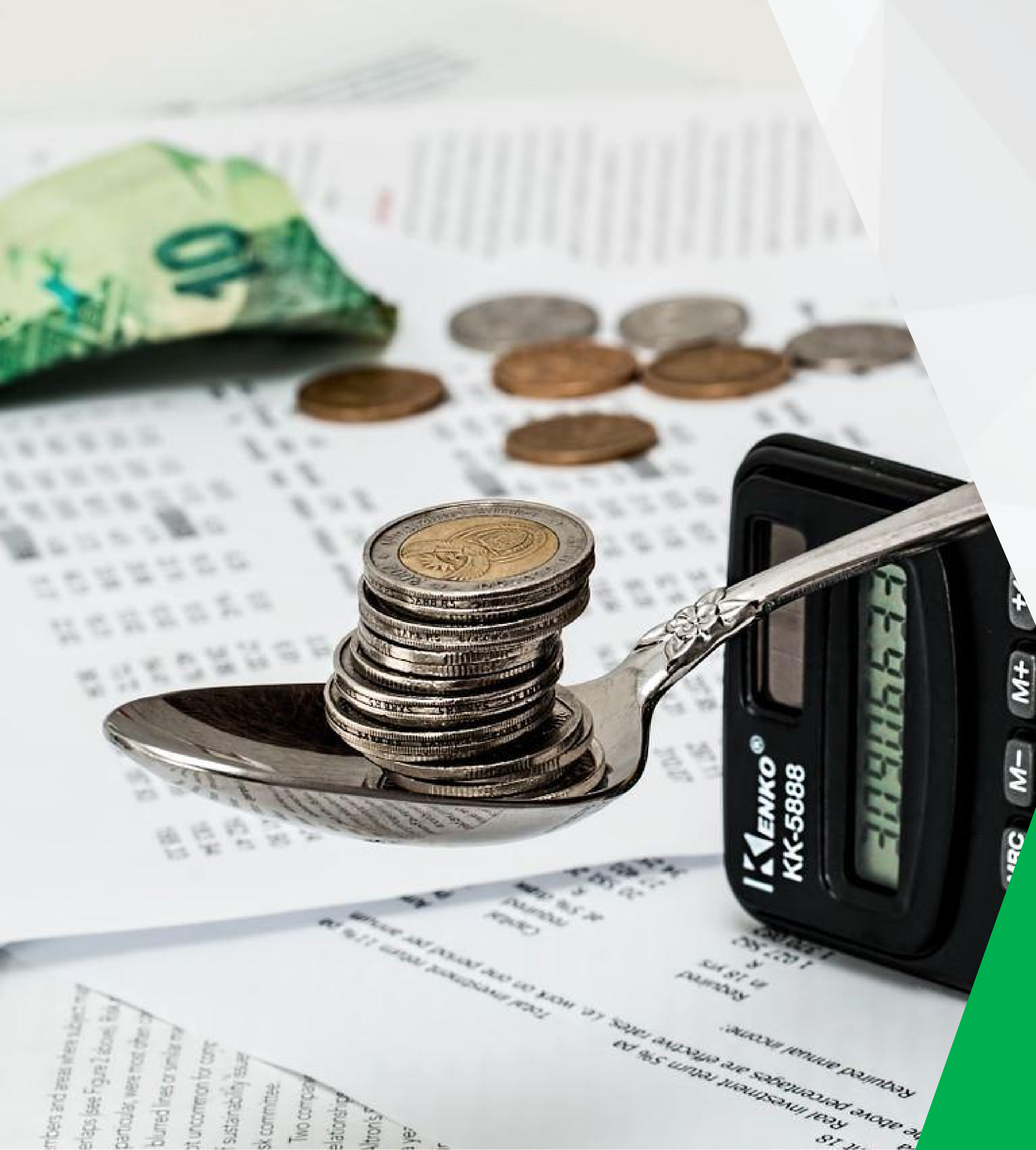
Prevention and Control of Fraudulent Transactions

Risk Control Dept.

February 24, 2022



Oceanpayment

01

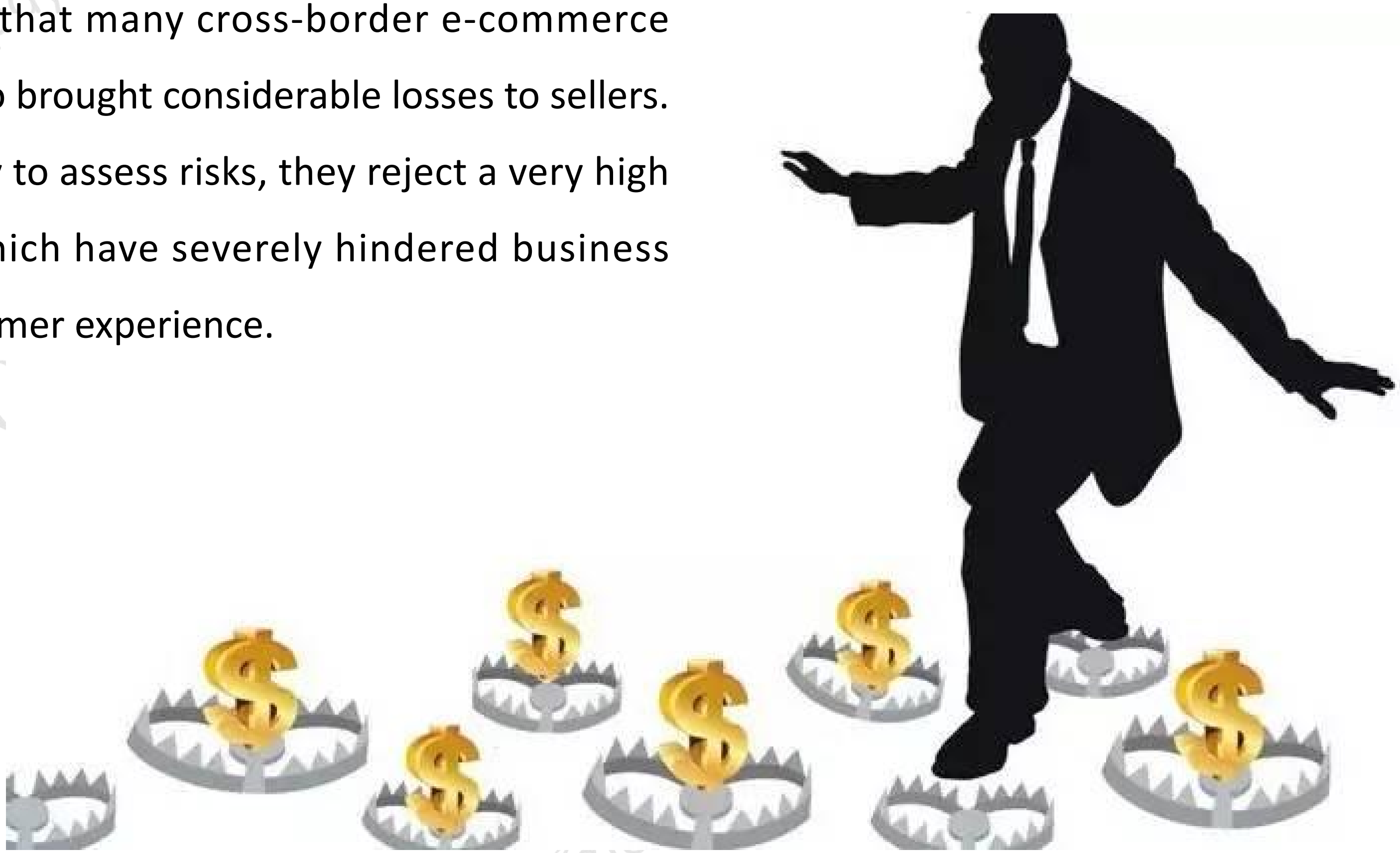
Why Preventing Fraudulent Transactions Is a Critical Necessity

Fraudulent transactions severely hinder sellers' development and negatively impact consumers' experience.

Oceanpayment

- Cross-border payment fraud is a problem that many cross-border e-commerce businesses have encountered, and it has also brought considerable losses to sellers.
- Moreover, since many sellers lack the ability to assess risks, they reject a very high proportion of normal customers, all of which have severely hindered business development and negatively impacted customer experience.

Due to a lack of manpower and resources, **small and medium-sized sellers** find it difficult to establish a comprehensive risk control system. As a result, they are more likely to become targets of fraudulent traders. So, are there any strategies to reduce such risks?



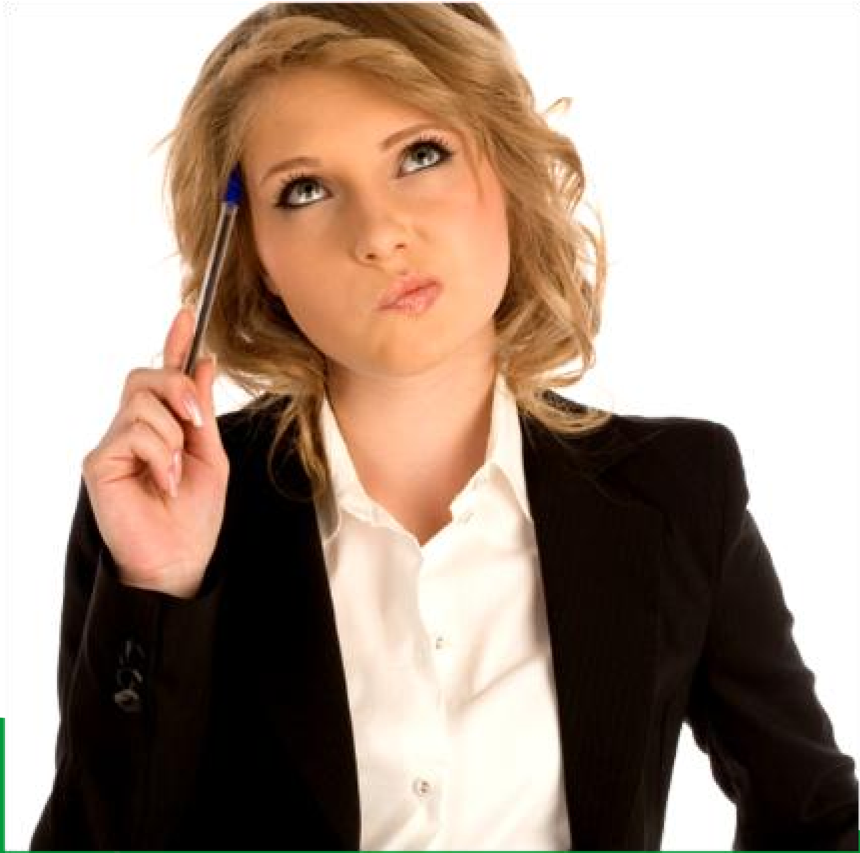
What is Chargeback

Credit Card Chargeback

A chargeback is the reversal of financial transaction,typically initiated by a customer(the cardholder),who disputes a sale on his or her credit card.

Time Frame

Generally occurring within 180 days after the transaction, some industries, such as aviation industry, and issuers can accept chargeback applications for a longer period of time.



Visa Chargeback Assessment Standard

Visa Dispute Monitoring Program (VDMP)

Level	VDMP
Level 1 (Early Warning)	0.65% and 75 chargebacks
Level 2 (Standard Program)	0.9% and 100 chargebacks
Level 3 (Excessive Program)	1.8% and 1000 chargebacks

Visa chargeback rate calculating method:

Visa Chargeback Rate = Count of Visa Chargeback of current month / Count of Visa success orders of current month

MasterCard Chargeback Assessment Standard

Excessive Chargeback Program (ECP):

Excessive Chargeback Merchant (ECM)

High Excessive Chargeback Merchant (HECM)

Level	New Assessment Standard
ECM	1.5% and 100 chargebacks
HECM	3% and 300 chargebacks

MasterCard chargeback rate calculating method:

MasterCard Chargeback Rate = Count of MasterCard Chargeback of current month / Count of MasterCard success orders of last month

If a merchant exceeds ECM standard, and the acquirer delays submitting the merchant’s ECM rectification report to MasterCard, the card organization will charge the acquirer an assessment fee of 500 USD per day for the first 15 days after the deadline, and then 1000 USD per day thereafter until the acquirer finally submits the ECM rectification report.

Oceanpayment

02

Strategies for Reducing Fraud Risks

Keep the Software Updated in Sync.

Many small and medium - sized sellers opt to use third - party website - building software or platforms to establish their online stores. Website - building service providers themselves attach great importance to preventing fraudulent traders. As a result, they frequently upgrade the website - building software to avoid vulnerabilities in it that could be exploited by hackers.

What sellers need to do is keep the software updated in sync.

Encourage consumers to set complex passwords

Set a complex account password

To prevent fraud arising from consumers' account theft, sellers can encourage consumers to set complex passwords when creating website accounts, thereby reducing the risk of account compromise. For instance, sellers could require consumers to create passwords using a combination of uppercase and lowercase letters, symbols, and numbers.

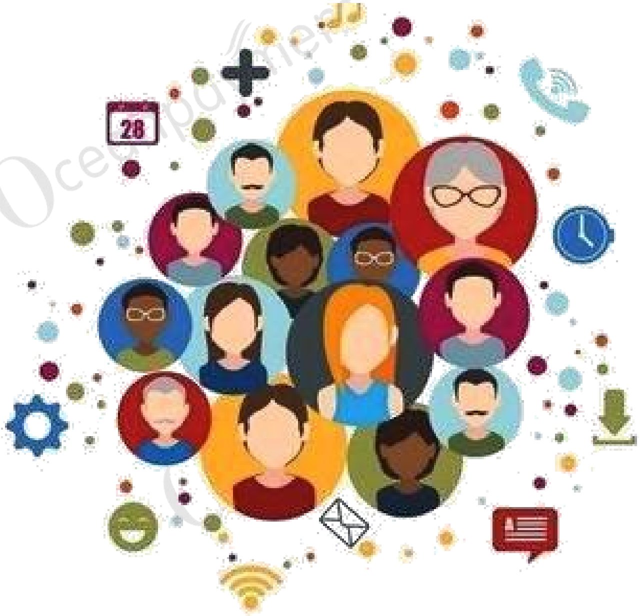
Password protection

Moreover, it's highly recommended that sellers prompt consumers to provide certain security - pertinent details during the account registration phase. For example, they could ask for the name of the kindergarten the consumer attended or their birthplace. In this manner, when consumers forget their passwords or their accounts are compromised, they can regain access to their accounts by answering these pre - set verification questions.

Know your customers comprehensively

- Sellers offer different products or promote their businesses in distinct regions, which means they face different consumer groups. Each group exhibits unique consumption characteristics. Based on these characteristics, sellers can capture abnormal situations and thus identify fraudsters.

- Fraudulent orders often involve bulk purchases of products, and the buyers show no preference regarding size, color, design, model, etc. Sellers should be cautious when accepting such orders.

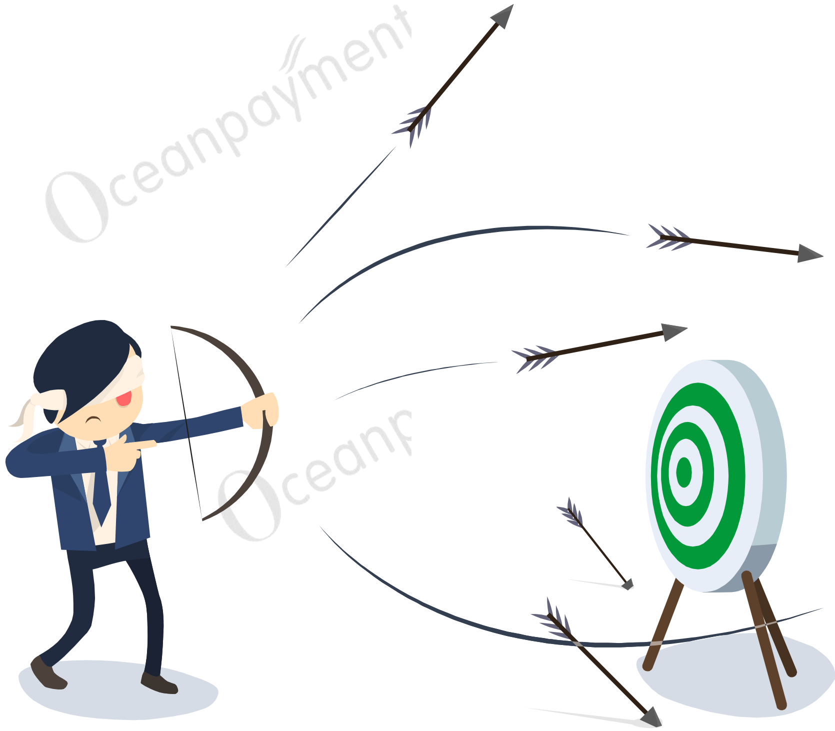


Pay attention to high - frequency orders

- Typically, fraudulent orders tend to target products that are easy to liquidate, as identical products are more convenient for fraudsters to convert into cash. Therefore, if the same consumer places multiple orders for the same product within a short period, sellers are advised to exercise caution when accepting such orders.

- Fraudsters usually attempt multiple online payments to verify the reliability of credit card information. This process often fails due to reasons such as risk control measures or mismatched bank information. It is normal to have one or two failed attempts before a successful transaction. However, if there are a large number of failed attempts before a successful one, sellers should be on high alert.

- Sellers can set a limit on the number of repeated orders. Once this limit is reached, the consumer's account will be locked, and they will be unable to use the shopping cart. The consumer will then be required to contact customer service to verify their identity before completing the purchase.



Implementing 3D Secure for High-Priced Goods

Oceanpayment

- Normally, fraudulent orders tend to cluster around high - value products, as these can bring fraudsters greater profits. When a single consumer's transaction amount is excessively high or they frequently purchase different high - value products, sellers are advised to exercise caution when accepting such orders.

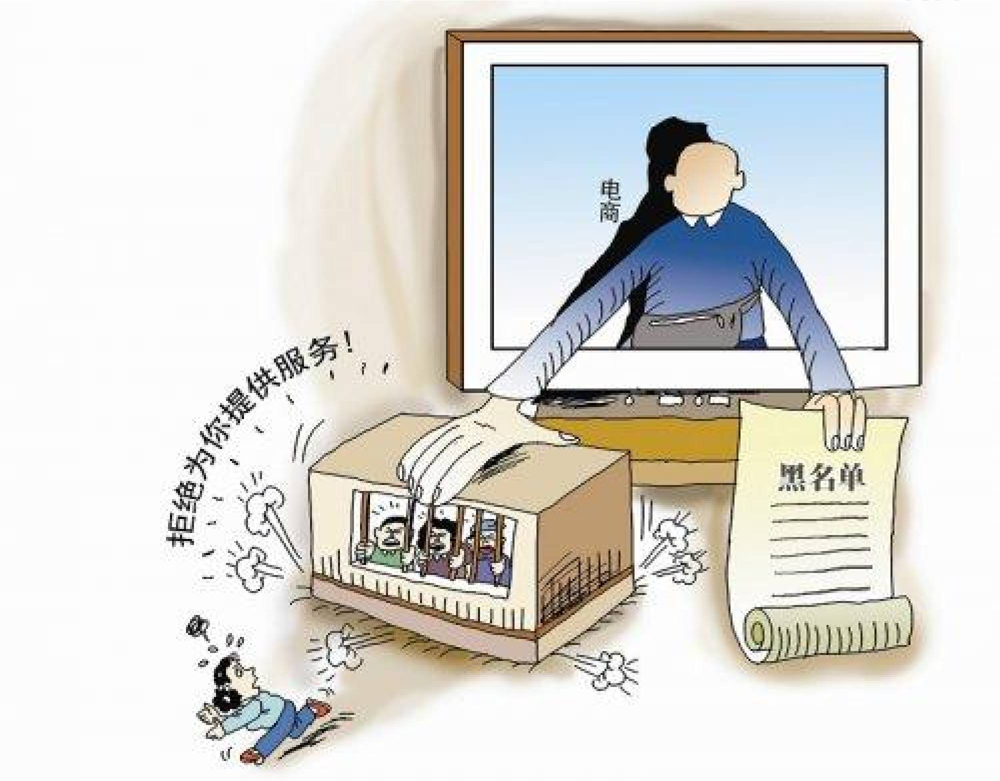
- In addition, for products with relatively high unit prices, sellers can also set up 3D Secure verification for credit cards to prevent chargebacks due to consumer fraud.

Confirm abnormal transactions via phone call

- It's important to note that not all abnormal transaction signals can be immediately identified as fraudulent behavior. In cases of uncertainty, sellers can contact the consumer via the phone number they've left, communicate with them, and verify the relevant order information.

- Often, fraudsters won't leave a genuine contact number. Therefore, this method can be an effective way to check the consumer's identity.

Establish fraud blacklist



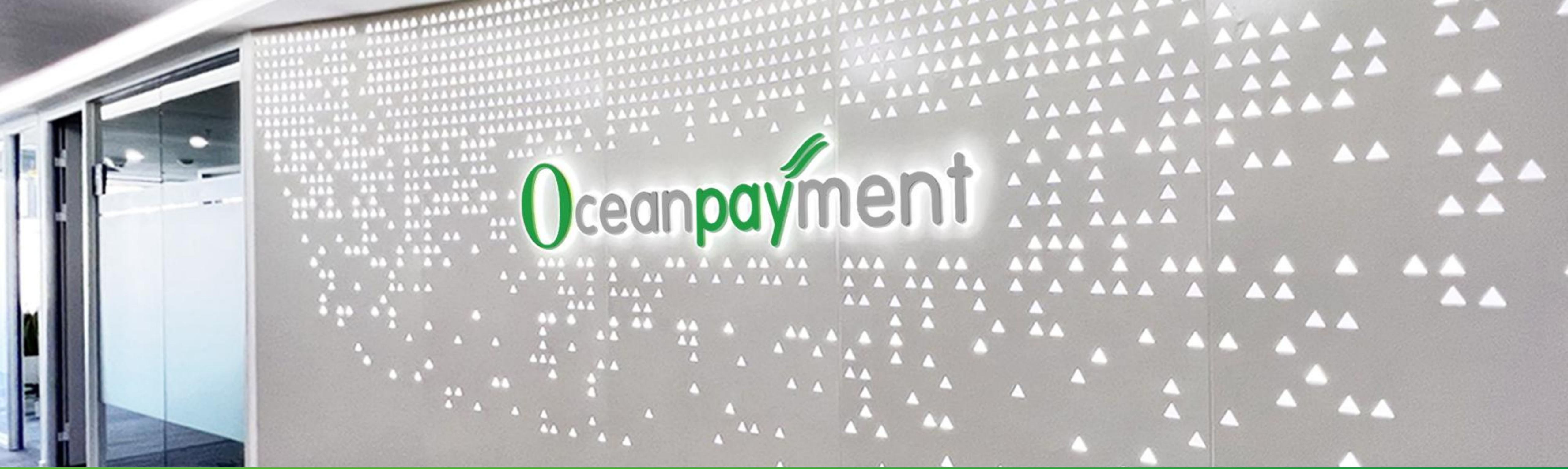
If a fraudulent order has been confirmed, all information related to this order should be documented. In subsequent transactions, once the same customer information appears, sellers need to block such transactions accordingly.

Select a professional cross-border payment provider to collaborate with

Oceanpayment

- In reality, identifying fraudulent traders is an exceedingly complex and specialized task. **For sellers, the optimal strategy is to partner with a trustworthy cross - border payment service provider to help manage transaction risks.**

- Oceanpayment's intelligent risk control system is capable of precisely identifying abnormal transactions by conducting multi - dimensional analysis and big - data matching based on the characteristics of various transaction risks. This enables it to promptly detect fraudsters and safeguard sellers' transaction security.



THANK YOU

扫一扫，
让全球支付更简单

info@oceanpayment.com.cn
HK@oceanpayment.com
www.oceanpayment.com
+86 4006 290 296