verifone

www.verifone.com

Infographic

How to Manage False and Fraudulent Chargebacks

In today's eCommerce environment, merchants and shoppers expect nothing less than a smooth and safe digital experience. With the growth of digital commerce come serious security challenges that every merchant has to confront to keep a safe environment for its business and shoppers. Managing fraudulent chargebacks is one of these security concerns that online businesses must continuously adress. Here is what you need to know.

What are fraudulent chargebacks?

A fraudulent chargeback occurs when an illegal transaction is initiated by someone who stole a credit card and the official cardholder disputes the fraudulent purchase, or when a shopper intentionally abuses their chargeback rights to both retain a purchased item and get their money back.

Use address verification systems as fraud prevention tool

AVS is a transaction security measure, used extensively in the United States, that helps merchants prevent fraud. It works to verify if the cardholder's address is correct or invalid, based on the card's billing address that is registered in the bank's files. AVS is a very helpful security tool to reject potentially fraudulent transactions.

Comply with PSD2

This is a set of laws for payment services, that aims to make the European payments market safer by protecting its users against fraud. PSD2 offers a wider layer of protection via Two Factor Authentication. To protect the confidentiality of end customer's security credentials, each online purchase within the European Economic Area must pass the 2FA process.

Implement 3D Secure 2.0

The latest technology version of 3D Secure, 3DS2 allows merchants to verify transactions with the cardholder's issuer, enabling banks and merchants to share rich data in the background.

After a shopper places an order, the transaction is processed by the issuing bank that will either approve or deny the transaction, based on the customer's information. This information is checked, and the resulting data is sent right back to the merchant.

Ask for card security codes

The card security code is featured on each card, a code of three or four digital numbers that help authenticate online transactions. This CCV code is collected by the merchant/provider along with the rest of the card details and sent directly to shopper's bank for authentication. If any issue occurs, the bank cancels the transaction.

Offer flawless customer service

Make sure your contact channels are easily accessible and visible. Communicate with users about any issue, whether it is technical or just a misunderstanding due to communication and notify your shoppers when you experience setbacks that could affect their transaction's processing and delivery.

Always confirm the delivery

Delivery confirmation is a helpful tool for merchants, as it provides useful information about the order's status, such as the exact date and time the purchase has been made, and when and how it will be delivered. This mechanism will boost your shopper's confidence in your services and potentially flag fraudulent orders.

Review your transactions

Review your older sales to see if there are suspicious transactions or upset buyers with orders that require a partial or full refund, to avoid chargebacks. When in doubt, ask your payment provider for assistance with your fraud review.

Takeaway

Managing fraudulent chargebacks is a serious and complex ongoing project, but it is not an impossible task. As a payment processor with integrated services, Verifone can help merchants implement fraud prevention tools, such as card and address verification systems, pre-authorization, and dynamic 3DS to keep their business protected.

verifone

The payments architects who truly understand commerce

www.verifone.com