Chargeback fraud: prevention and response

Introduction

Chargeback fraud occurs when a business provides a product or service to a customer who has used stolen card details to make a purchase. After receiving the goods or services, the legitimate cardholder will find out that a fraudulent purchase has been made. They then dispute the transaction through their bank, resulting in a chargeback that reverses the payment. This then leaves the business without the product or payment. It exploits the chargeback system meant for genuine errors or unauthorised charges, causing financial and reputational damage to merchants.

This fact sheet will first cover the immediate response to chargeback fraud, then discuss methods for preventing this from occurring in the first place.

Immediate response

If your business has encountered a fraudulent chargeback incident, you can:

☐

1. Challenge the chargeback

You may be able to challenge the chargeback with supporting evidence with the payment processor. Supporting documentation may include the following:

- Proof of purchase
- Terms and conditions of sale
- Customer's signature or delivery information
- Shipping documents
- Invoice details

☐

2. Raise a complaint with AFCA (where needed):

You may complain to the Australian Financial Complaints Authority (AFCA) if your payment provider:

- Did not follow the proper chargeback process
- Gave you incorrect information
- Treated you unfairly in relation to your merchant facility agreement

NOTE: *AFCA cannot force Visa, Mastercard or EFTPOS to overturn a chargeback. AFCA's role is to review how your bank/payment provider handled your case under your contract and relevant rules.*

Prevention methods

☐ Recovery of the charged back funds is unfortunately often unreliable. The best way to combat fraudulent chargebacks is to remain scam aware and implement payment protection measures. IDCARE recommends implementing 3D Secure 2.0 (3DS2) authentication for online payments (more information below).

Staying scam aware – chargeback red flags

☐ Be aware of customers who:

- Provide credit card details over the phone
- Attempt to pay with multiple credit cards once one fails to process
- Are looking to purchase large or expensive orders without providing many details about themselves or their company
- Are not willing to pick up the order themselves or interact in-person
- Are not contactable easily or cease contact after placing the order.

☐ While these 'red flags' may not always mean a customer is planning to initiate a fraudulent chargeback, they should serve as points of suspicion and potential early warnings. With all customer interactions, **document everything** so that, in the event of a fraudulent chargeback, disputing the chargeback with the payment processor is supported with evidence. To support this, we recommend **placing tracking** on orders to verify that the customer did receive the item/s.

3D Secure 2.0

What is 3D Secure?

☐ 3D Secure 2.0 is an additional security protocol that lets the cardholder's bank verify the customer during checkout (e.g. via SMS code, banking app, or biometrics). The latest version, 3D Secure 2.0 (EMV 3D Secure):

- Improves customer experience with frictionless verification flows
- Helps reduce cart abandonment
- Potentially shifts liability for fraudulent transactions from the merchant to the card issuer

☐ While 3D secure does not guarantee 100% prevention against chargebacks, it reduces the number of fraudulent chargebacks and protects merchant rights.

NOTE: *The card-holder's issuer (bank) and the card network must support 3DS for that card. If the issuing bank isn't enrolled in or configured for 3DS, then you won't get the full protection.*

How to enable 3D Secure 2.0

☐ Some payment processors have 3DS2 enabled by default, and others may require you to turn it on manually. Contact your payment provider to confirm 3DS2 is enabled for all your online transactions.

Cost of 3D Secure 2.0

☐ Payment providers often include 3DS2 in normal card processing fees. Some bank merchant facilities may charge a setup or monthly fee. Check with your provider for details.

For additional support or information, contact IDCARE:

Submit Get Help Form | 1800 595 170 (Aus) | 0800 121 068 (NZ)