

How to prevent eCommerce fraud

eCommerce fraud is a widespread and potentially devastating threat to large and small online businesses alike.

Here's what you need to know.

Every \$1 of fraud loss can cost your company \$3.13.

news.cardnotpresent.com/news/lexisnexis-study-preview-finds-cost-of-fraud-for-ecommerce-merchants-highest-ever



60% of small businesses are out of business within 6 months of a cyberattack.

inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself

Types of eCommerce Fraud

- Card Testing**



Criminals use stolen card numbers to run small transaction amounts (e.g., \$.01) to see if account numbers are still valid, which could also result in substantial authorization fees.
- Stolen Credit Card Fraud**



Cybercriminals use stolen card information to make large-ticket purchases online and ship the items to a reshipper for collection.
- Friendly Fraud (or Chargeback Fraud)**



A customer falsely claims a product was never delivered and asks for a refund.
- Merchant Identity Fraud**



Fake merchant accounts are set up so criminals can run fraudulent transactions, collect the funds, then close the account.
- Account Takeover Fraud**



Cybercriminals gain access to a customer's login credentials to use stored credit cards to purchase goods and ship them to an updated address.
- Overpayment Fraud**



Criminals intentionally overpay with stolen credit card info, then ask for a refund to be paid to another account.

9 Ways to Minimize eCommerce Fraud

Implementing or refining each of these will help prevent fraud and give your legitimate customers greater confidence to make purchases.

- 

1 Be Tough on Passwords — Require customers to use passwords and change them at regular intervals. Strong passwords should be between 8 – 10 characters, including numbers, symbols and upper/lower case letters.
- 

2 Convert to HTTPS — An HTTPS site is recognized by users as being safe. It will help to attract legitimate customers and deter criminals.
- 

3 Have a Secure Platform — Use a proven eCommerce platform with the necessary security features, including SSL certificates and an encrypted payment gateway. Keep your platform and software up-to-date.
- 

4 Install Fraud Protection Tools — These include Address Verification Service (AVS) to confirm that the address and zip code given by the customer matches the billing data, velocity filters to deter card testing, card verification value (CVV) filters to confirm 3-digit code on back of card matches what the card-issuing bank has on file, and unmatched refunds filter to confirm refund is issued back to the card that was used for the initial sale.
- 

5 Monitor Suspicious Transactions — Review small-order authorizations and sales carefully. Card testing accounts for 16% of all eCommerce fraud.*
- 

6 Encrypt Data — Encryption technology uses algorithms to encode credit card information, making it unreadable to cybercriminals. Only the payment processor can decrypt the data and decipher the payment details.
- 

7 Utilize Tokenization — This advanced security method minimizes a merchant's liability by replacing a credit card number or other sensitive information with random, non-specific IDs or "tokens." This eliminates the need to store customers' account numbers.
- 

8 Use Two-Factor Authentication (2FA) — Customers use two means of identification to access their account, one of which is usually a temporary code sent to a certified mobile device.
- 

9 Maintain PCI Compliance — Compliance with Payment Card Industry Data Security Standards (PCI DSS) is required for every business that accepts credit cards. Card brand penalties and fines are steep for noncompliant entities that suffer a data breach.

*chargebackgurus.com/blog/effective-tools-strategies-to-prevent-card-testing-aka-card-cracking