

**5 TIPS
TO PROTECT YOUR
ONLINE STORE
FROM HACKERS &
CYBERCRIMINALS**



5 TIPS TO PROTECT YOUR ONLINE STORE FROM HACKERS & CYBERCRIMINALS



Surge in E-commerce Delivers Rampant Fraud

1. Curb Chargebacks or “Friendly Fraud”

One of the most expensive types of e-commerce fraud is chargebacks. This happens when dishonest customers ask for a refund from their credit card company after they claim they didn't receive something they ordered; the product wasn't as described online; or that it was damaged. Chargebacks are costly and take a lot of time to resolve. This is how you can curb the number of chargebacks:

- Follow your payment processing protocols for card-not-present transactions.
- Ensure billing and return policies are clear.
- Fight chargebacks by keeping meticulous shipping records and receipts.
Require people to sign for packages.
- Encourage customers to resolve problems directly with you because refunds cost less than chargebacks.

2. Reduce Identity Theft

If you don't safeguard customer information, hackers will steal it and use the stolen data to make illegal purchases. This is the most common type of e-commerce fraud. To reduce ID theft:

- Ensure you are compliant with the Payment Card Industry's guidelines for storing payment card data.
- Keep your platforms and software up to date.
- Install and regularly update anti-malware and anti-spyware software to fight attacks.
- Implement a CAPTCHA to stop bot attacks at checkout.
- Require a zip code or postal code to stop fraudulent purchases.
- Demand customers create strong passwords that include numbers, letters and symbols.

3. Lower the Return Rate

Experts estimate people [return 15% to 40%](#) of what they buy online, compared to 5% to 10% of in-store shopping. Since picking, packing and delivery rates can be so costly, consider adding 'buy online and pickup in-store' (BOPUS) service. Since the pandemic, BOPUS sales are up 259% over last year. An Adobe study found customers like the satisfaction of receiving their item immediately instead of waiting for it to arrive in the mail. The study found 30% of online consumers prefer using BOPUS or curbside over delivery – and were less likely to return the item.

4. Two-factor Authentication

Require customers to provide at least two means of confirming their identity and purchases. This is something we at [Red Maple](#) highly recommend as this extra step gives consumers confidence that you're taking security seriously and reduces the chances of chargebacks.

- Use address verification to ensure a customer's credit card billing address in checkout matches the address with the issuing bank.
- Require customers to provide the Card Verification Values or Codes (CVV or CVC). This is the three or four digit number on the back or front of credit cards. Doing this makes the sale more secure. By requiring the CVV/CVC code, it's more likely the person has the credit card with them.

Red Maple also offers a product called Advanced Credit Cards, which is a Microsoft Dynamics credit card processing extension that securely accepts and processes credit card payments. [Click here to learn more.](#)

5. Know your Customer

Keep a close eye on user behavior with fraud-detection tools. Consumers often order the same products, spend the same amount of money, and ship to the same address. [The Merchant Fraud Journal](#) reports a spike in spending is a good indicator that an account has been hacked.

- Verify new, large, and suspicious orders from overseas by calling customers to verify identification.
- Set limits on the dollar value and number of products purchased by each customer to minimize your exposure to fraud.
- Ensure your contact information, including your phone number, is prominent on your website.
- Provide excellent customer service. Customers are less likely to contact their bank for a chargeback if the business has clear return policies and contact information on their website.

While it's exciting that a new Adobe report found the pandemic has driven e-commerce to levels previously expected in five years, it's critical to understand fraudsters are also upping their game to steal some of that money. Following the best practices above can help ensure legitimate customers are buying your services and products.

