Preventing Card-Not-Present Fraud

Tips to help reduce the risk of online fraud

AMERICAN EXPRESS

DON'T *do business* WITHOUT IT™

Online sales are on the rise. With that trend, however, comes a potential increase in online or card-not-present fraud.

American Express is here to help you protect your business and customers from fraud with useful information and tips.

FRAUD HAPPENS

88%

OF MERCHANTS

reportedly experienced fraud in 2022.*

Common Types of Card-Not-Present Fraud

Fraudsters are constantly developing new techniques to defraud merchants and their customers. **Here's some of the most common techniques:**

- **Phishing:** when fraudsters pretend to be you and send communications to your customers.
- **Identity theft:** when a customer's personal information has been stolen.
- **Compromised payment credentials:** when a fraudster uses stolen card numbers to make online purchases.
- **Account takeover:** when a hacker gains access to account credentials, such as username or password.
- **Malware:** when malicious software is loaded onto your company's systems.
- **Location masking:** when fraudsters hide or change their true location to circumvent your security and app features.

Continue reading for tips to help you prevent fraud.

To learn more about how to help protect your business, visit **americanexpress.com/fraud-solutions** and **americanexpress.com/datasecurity**.

*Source: The Amex Trendex: 2022 Payment Security Edition is based on a sample of 411 business leaders in the U.S. who have responsibility for making decisions regarding customer payment options, IT/data security or online sales strategy and planning. The sample for the study came from an online panel. Fieldwork was conducted September 15 – 25, 2022.

How to Help Prevent Fraud in Your Business

You can’t prevent fraudsters from attempting to compromise your data security, but you can take some important steps to help protect you and your valued customers.

Here’s what to look out for:

- ✓ Larger-than-normal orders.
- ✓ Orders with multiple big-ticket items.
- ✓ Orders that use multiple cards but share the shame shipping address.
- ✓ Orders that use multiple cards and a single IP or email address.
- ✓ Orders shipped to international addresses.

Best Practices:

- ✓ **Validate your data security** using the Payment Card Industry Data Security Standards (PCI DSS). These guidelines provide a baseline of technical and operational requirements that can help you build a strong data security foundation.
- ✓ **Remember that American Express will never ask you to provide your personal information** over the phone or via text or email. Also encourage customers to type in your website address instead of clicking on links.

Online Orders:

- ✓ **Capture and use as much information as possible**, such as email, IP address, billing/shipping information and security code/4-digit CID.
- ✓ **Require your customers to set up an account** versus offering guest checkout.

Telephone Orders:

- ✓ **Direct customers to an online/digital channel** to enter payment and billing information.
- ✓ **Ask customers for additional information** to help validate them.

To learn more about how to help protect your business, visit **americanexpress.com/fraud-solutions** and **americanexpress.com/datasecurity**.