CARD NOT PRESENT FRAUD

Online sales are on the rise. With that, fraud is also on the rise. Merchants estimate fraudulent transactions account for an average of 27% of their annual online sales, a significant increase from 18% in 2018.*

Why is Card Not Present fraud growing?

Online fraud has grown over the last 10 years as a result of several factors:

- Growth in e-commerce and global acceptance of EMV Chip Cards
- Omni-channel Merchant environments have led to new ways to make payments, but has also created new ways for fraudsters to commit fraud attacks.
- Fraudsters constantly develop and promote new techniques and tools.

Types of Fraud that commonly occur online:

- Phishing
- Identify theft
- Compromised payment credential (e.g. fraudster uses stolen card numbers to make online purchases)
- Account Takeover
- Malware
- Location masking

Preventing Card Not Present Fraud

Protecting your business from fraud is important. There are things you can do to help prevent fraud.

- Capture and use as much information as possible. For example, Email, IP address, billing/shipping information, and security code/4-digit CID.
- Require customer to set up an account rather than using guest check-out.
- Visit **americanexpress.com/fraud** to view more tips.

When processing online transactions, use extra care if you notice:

- Larger than normal orders
- An order with many big ticket items
- Shipping to an international address
- Transactions placed on multiple cards but all shipping to a single address
- Multiple cards used from a single IP or email address

Telephone/Mail order can bring an increased risk for fraud

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

* Source: American Express Digital Payments Survey