onbe™

Spot the Fraud

The 5 most common fraud risks businesses face

According to US Federal Trade commission data, consumers saw a 30% increase in fraud losses from 2021 to 2022, a reported $8.8 billion. Lacking adequate fraud, security, and compliance controls can lead to significant financial losses, a damaged reputation, and the loss of customer trust. With the rising prevalence of sophisticated identity theft, friendly fraud, and phishing techniques, companies are finding it more difficult to meet the stringent regulatory demands to combat fraud in the payments industry.

By understanding today's most common forms of payment fraud along with the best practices for minimizing risk, businesses can protect themselves and their recipients:

1 ACCOUNT TAKEOVER

Account takeover is when a malicious third party gains access to a user's account credentials. Be alert for unusual account activity, such as multiple failed login attempts, sudden changes in account details, or a batch of newly opened accounts with similar personal information.

Prevent account takeover by implementing strict verifications or systemic checks for account changes. For high-value transactions, require authentication or identity confirmation.

2 CARD NOT PRESENT (CNP)

CNP transactions are fraudulent, lower-dollar e-commerce transactions that can easily fly under the radar. Because they aren't high value, these transactions may be overlooked or ignored by cardholders.

CNP transactions can be domestic or international. The merchant naming convention is typically unusual or a deliberate manipulation of a well-known brand.

3 FRIENDLY FRAUD

Friendly fraud is when a cardholder falsely identifies a purchase on their transaction statement as fraudulent.

To mitigate friendly fraud, keep detailed records of customer transactions, interactions, and delivery, as well as customer service records for evidence in case of disputes. Proactively verify customers with best practices such as Know Your Customer (KYC) processes, and monitor customers with a history of frequent chargebacks or those who immediately request a chargeback after a transaction without contacting the business first.

4 PHISHING

Phishing is the practice of posing as a reputable person or organization to persuade individuals to share personal information.

Take action by training employees to recognize phishing emails, suspicious URLs, and unsolicited phone calls or emails requesting access to sensitive information. Establish clear communication protocols to verify the identity of individuals requesting sensitive information or account actions.

5 ENUMERATION ATTACK

Enumeration attacks are when bad actors attempt to gain brute-force access to web applications, often using credentials exposed in previous breaches or phishing scams.

Monitor for sudden spikes in transaction volume, high numbers of chargebacks, or transactions with unusual dollar amounts.

Without proper safeguards in place, businesses are vulnerable to unauthorized transactions, data breaches, and account takeovers—all of which come with potential regulatory fines. To mitigate these risks, it's crucial for businesses to implement comprehensive fraud detection and prevention methods, including multi-factor authentication, robust transaction monitoring, and thorough Know Your Customer (KYC) and Know Your Business (KYB) processes. By proactively addressing threats and protecting themselves against bad actors, businesses can ensure the security and integrity of their payment programs, maintain customer trust, and protect their bottom line.

OnbeGuard, the latest enhancement to Onbe's suite of fraud prevention tools, uses machine learning-supported Behavioral Biometrics that generate alerts, progressive modeling, and proactive fraud identification to predict and combat fraud—so you can be ready to deliver secure, seamless payment experiences.

Contact us to learn more about OnbeGuard.