ACI Worldwide
Real-Time Payments

Defeating COVID-19-Inspired Fraud

Protect your business and your customers during this uncertain time.

Increasing Online Traffic

The closure of many brick-and-mortar stores has already driven an uptick in online traffic.

This has led to increased opportunities for fraudsters.

Phishing

Banks have already begun warning of an increase in phishing.

Phishing involves official-looking emails or other communications asking for personal/sensitive information.

Fraudsters obtain this information to acquire goods online or open fraudulent accounts.

Two Phishing Typologies

Account Takeover

Fraudsters gain access to accounts, locking out the true account owners while draining the accounts.

Synthetic Fraud

Fraudsters combine stolen, real information with fake information to create fraudulent accounts.

Friendly Fraud

Friendly fraud involves customers charging back goods that were legitimately ordered and received.

Fraud patterns here may take longer to emerge.

Banks, due to personnel limitations, may take longer to confirm fraud or chargebacks.

Remaining Vigilant

- Customers and merchants must work to ensure their safety.
- Raise inquiries with banks on any onerous transactions.
- Pay careful attention to very low-value purchases, as they are a good indicator of fraud.
- Merchants are encouraged to immediately raise queries with risk teams at the first sign of trouble.
- The ACI risk team is skilled in assessing data and patterns and can quickly help expose new fraud threats and mitigate fraud exposure.

Want to Know More?

Please contact merchantpayments@aciworldwide.com.