KeyBank

Commercial Card Fraud Prevention

Understanding fraud schemes, recognizing red flags, and mitigating risk.

Fraud scheme	How it happens	Red flags	Mitigation
Card Not Present (CNP) fraud Unauthorized use of a card for online, phone, or mail transactions where the physical card is not required.	• Compromised card data from merchant or breaches • Phishing or malware capturing card credentials	• Small test charges followed by larger purchases • Multiple transactions at unfamiliar merchants • Purchases outside normal geography or business hours	• Merchant Category Code (MCC) restrictions • Real-time transaction alerts • Virtual cards for online vendors • International spending does not need to be on every card
Lost or stolen card fraud A physical card is stolen or misplaced and used before it's reported.	• Cards lost or taken from vehicles, hotels, or shared offices • Mail theft of newly-issued cards	• In-person purchases outside employee travel patterns • Rapid spending shortly after card issuance	• Spending limits by cardholder • Immediate self-service card freeze • Chip and PIN enforcement where possible
Employee abuse An authorized employee uses a commercial card for non-business or prohibited purposes.	• Weak expense policies • Lack of receipt review or reconciliation • Shared cards without accountability • Cash advances	• Repeated charges just under approval thresholds • Personal merchants (retail, entertainment, food delivery) • Missing or generic receipts	• MCC restrictions • Clear card use policies • Required receipts and coding • Manager approval workflows • Analytics to identify out-of-policy spending
Merchant collusion An employee and merchant conspire to inflate charges or run unauthorized transactions.	• Manual card entry by the merchant • Authorized party conspires with merchant so that they both benefit	• Repeated round dollar transactions • Unusual frequency with a single merchant • Charges inconsistent with goods/services received	• Transaction detail level (Level II/III data) • Periodic vendor reviews • Separation of purchasing and reconciliation duties

Tips for protecting your business from commercial card fraud

First line of defense

Transaction-level controls

Prevent or stop fraud at authorization by limiting where and how a card can be used.

- MCC restrictions to block non-business or high-risk merchant types
- Dollar and velocity limits (per transaction, daily, monthly) to reduce exposure if credentials are compromised
- Geographic and currency restrictions, especially for international or cross-border transactions
- Virtual cards (single-use or vendor-locked) to prevent reuse of stolen card numbers and limit merchant-side breaches
- Enable PIN creation for all transactions

Account takeover (ATO) prevention

Authentication and access controls

Reduce ATO and portal-based fraud.

- Multi-factor authentication (MFA) for card portals and expense platforms

  Note: Two-step verification for transactions is coming soon.
- Role-based access controls limiting who can add users, change limits, or view full card numbers
- Periodic user access reviews to remove outdated or excessive permissions

Detection layer

Monitoring, alerts, and analytics

Identify fraud quickly, reducing loss severity.

- Real-time transaction alerts for cardholders or program administrators (for example, text message alerts)
- Suspicious activity alerts for program administrators
- Issuer fraud scoring and anomaly detection, including network-level analytics (for example, Visa authorization scoring)
- Monitoring for behavioral anomalies such as new merchants, test charges, or rapid spending changes

Internal fraud reduction

Cardholder and program controls

Address friendly fraud and employee misuse, which are persistent loss drivers.

- Clear commercial card use policies defining permitted and prohibited spending
- Receipt requirements and coding standards to support reconciliation and review
- Manager approval workflows for exceptions or higher-risk spend categories
- Spending analytics to identify threshold avoidance, personal merchants, or out-of-policy behavior

Example: Airline scam

A fraudster uses stolen commercial cards and CNP transactions to buy high-dollar, fully refundable tickets for same-day or next-day flights. Then, they sell the ticket for crypto or cash, use the ticket, get a refund for cash, or put it into a travel wallet.

How you can protect your business

- MCC restrictions and transaction controls for airline purchases
- Real-time transaction alerts for cardholders or program administrators
- Monitoring for behavioral anomalies such as same-day or next-day flight purchases

KeyBank