Fortis + VISUAL MATRIX™ Hospitality Operating Platform

‘Tis the Season for Holiday Chargebacks

The Fortis Guide to Keeping Your Hotel Protected

The holidays bring full rooms, fast-paced check-ins, and packed reservation logs. But they also bring a rise in fraudulent charges, processing errors, and costly chargebacks.

Whether it’s guests disputing charges after checkout, stolen cards sneaking through during rush hours, or third-party reservation confusion—the risk is real, but preventable.

This guide walks you through practical, hotel-focused strategies to reduce chargebacks during the holiday season and stay protected with support from Visual Matrix and Fortis.

Why **Chargebacks Spike** During the Holidays

1

Friendly Fraud (most common)

Guests file chargebacks because they:

- Claim they canceled a reservation.
- Dissatisfied with room conditions or amenities.
- Say they didn’t authorize the transaction.

Often, these aren’t intentional scams. They result from poor communication, missing documentation, or the guest calling their bank before contacting the hotel.

2

True/Criminal Fraud

Fraudsters take advantage of busy seasons to:

- Use stolen credit cards
- Perform account takeovers
- Book through fraudulent third-party platforms
- Misuse virtual cards

3

Processing or Merchant Errors

In the holiday rush, hotel teams may:

- Charge the wrong amount
- Forget to capture signed receipts
- Charge beyond pre-authorization limits
- Duplicate or delay charges
- Fail to communicate no-show or cancellation policies

These are the easiest chargebacks to prevent, just with clear workflows and documentation.

ID Verification: Stop Fraud Before it Happens

Verifying identity is one of the most powerful ways to stop chargebacks.

Best Practices

- Always check the guest's government-issued ID and confirm the name matches the credit card.
- For third-party authorization forms, collect:
  1. Cardholder name
  2. Guest name (if different)
  3. Billing address
  4. Cardholder signature
  5. Card and ID images (securely submitted)
- Never check in a guest using a card that is not present unless a verified authorization form is in place.

Red Flags to Watch For

- Guest refuses to show ID
- Mismatched name on ID, card, or reservation
- High spending on extras early in the stay (gift shop, room service)
- Hesitation when asked to re-present their card

Tip: A simple ID check can save thousands in fraud and reduce nearly all post-stay disputes.

Payment Verification: Every Card, Every Time

→ Chip-Read the Card

- Always insert the card for an EMV chip-read. Tap-to-pay is allowed but offers less protection, especially for check-ins, extensions, or high-risk charges.
- Keyed entry should be rare and reserved for:
  1. No-show charges
  2. OTA virtual cards
  3. Verified third-party authorizations

→ Tap-to-Pay vs. Chip Read

- Tap uses EMV cryptograms—but chip inserts create stronger proof of card presence.
- For dispute protection, especially in hospitality, chip-read is preferred.

→ For Extended Stays

- Charge every 5–7 days
- Get a new signed authorization each time
- Provide a receipt after every charge

→ Online Hotel Collect Reservations

- Guests must present the card at check-in and it must be chip-read.
- Pre-authorizations are allowed in advance—but only chip-read protects you in disputes.

→ For Virtual Cards

- Do not charge incidentals or extra nights to the virtual card.
- Overcharges will lead to automatic chargebacks.

Documentation: Your Legal Defense Against Chargebacks

In a chargeback, the burden of proof is on the hotel. Strong documentation often determines whether you win or lose.

→ "Compelling Evidence" Includes

- Signed folios, receipts, authorization forms
- Proof of stay (emails, room numbers, key logs)
- Guest communications or satisfaction logs
- Cancellation confirmations
- Cardholder ID and card copies (where policy allows)
- Authorization approval codes or EMV proof

→ No-Show Charges

Card brands require:

- Charge posted the day after scheduled arrival
- "NO-SHOW" clearly written on receipt
- Cardholder's name (not guest's)
- Truncated card number
- Visible cancellation policy disclosures

→ Damage Charges

To charge for damage, gather:

- A clear explanation tying the damage to the guest
- Incident/police/insurance reports
- Comparison of insurance coverage vs. guest liability
- Guest signature authorizing the charge (after damage occurred)

Without these? You'll likely **lose** the chargeback.

Holiday Season **Chargeback Prevention** Checklist

Do This Every Time

- [ ] Clearly display refund & cancellation policies
- [ ] Use AVS & CVV for card-not-present transactions
- [ ] Process charges within 7 days of authorization
- [ ] Refund to the original card only
- [ ] Double-check tax rates and totals for virtual cards
- [ ] Never proceed with declined or suspicious cards

Train Your Staff on These Key Phrases

Extensions

"To protect your personal information, we don't store full card numbers. To extend your stay, please stop by with your card so we can chip-read it."

Cancellations

"Our cancellation policy requires a confirmation code. If you canceled, please provide it so we can verify the cancellation."

How **Fortis + Visual Matrix** Keeps Hotels Protected

Together, Fortis and Visual Matrix help hotels:

- Automate secure payment processing
- Stay compliant with lodging best practices
- Reduce fraud during occupancy spikes
- Avoid most no-show, virtual card, and cancellation chargebacks
- Equip staff with repeatable, error-reducing workflows

With smart systems and trained teams, even your busiest holiday season can be fraud-free and profitable.

→ Learn More about Fortis
→ Get the full Fortis Chargeback Guide

Fortis

+

VISUAL MATRIX™
Hospitality Operating Platform