



THE GROWING CHALLENGE OF CHARGEBACKS AND FRAUD IN THE HOTEL INDUSTRY

Abstract

The travel and hospitality industry is facing an ever-increasing threat from chargeback fraud, with fraudsters exploiting weaknesses in payment systems to threaten both financial stability and customer trust. The main reasons for chargebacks in the hotel industry include criminal fraud, customer disputes, authorisation issues, and processing errors, all of which can lead to costly chargebacks.

Hotels must adopt a multi-layered approach to combat this, involving advanced fraud detection tools, secure payment systems, and comprehensive employee training. Implementing strategies like AI-driven fraud prevention and industry-wide collaboration can also facilitate chargeback prevention, helping reduce vulnerabilities, protecting revenues, and improving customer satisfaction. As digital payments continue to evolve, proactive measures are essential for safeguarding the hospitality industry against chargeback [fraud in hospitality industry](#).



Hospitality businesses of all sizes, whether small inns or multinational hotel chains are one of the cornerstones of the global economy, with the hotel industry processing high volumes of low-value transactions. But these transactions, along with the growing prevalence of digital and credit card payments, have

left hotels vulnerable to chargeback fraud, disrupting both operations and financial stability. From identity theft and account takeover to friendly fraud, miscreants are finding sophisticated ways to exploit weaknesses in payment systems. Beyond the immediate financial losses, chargeback frauds also have long-term

implications for the continuity of business operations and customer satisfaction and trust. Hoteliers today must leverage technological innovation and adopt more robust strategies to navigate this growing challenge and protect themselves from these fraudulent activities.

The role of credit cards in consumer digital payments

Digital payments are now mainstream and increasingly embedded in daily life, even as they continue to evolve. The rise of digital payments has fundamentally reshaped consumer behaviour across industries, with credit cards remaining

central to this evolving landscape. The travel and hospitality industry is no exception, as credit cards account for the majority of transactions, whether for bookings, room service, or other on-site amenities. However, this increase in

credit card transactions has also resulted in increased numbers of chargeback disputes, making chargeback prevention a crucial step for protecting revenues and maintaining operational efficiency.

Reasons for chargebacks in the hotel industry

Originally intended to be a measure protecting customers against fraudulent transactions, chargebacks have now become a double-edged sword that can

disrupt the operations of a hospitality business. Understanding the specific reasons behind these chargebacks is essential for hoteliers looking to

implement effective chargeback fraud protection strategies. The primary chargeback triggers include:



Criminal fraud or fraudulent transactions

Criminal fraud is one of the most common triggers of chargebacks in the hotel industry. Fraudsters can use tactics like identity theft or account takeover to obtain credit card details of unassuming victims and test card limits with small

transactions to see if the card works before making larger purchases. Once the victims report this fraud, the hotels bear the associated financial loss. Without proper fraud detection and prevention systems in place, hotels remain vulnerable

to such tactics, making chargeback fraud protection and prevention strategies critical to minimise the damage caused by criminal fraud.



Customer disputes and cancellations

Customer dispute is another major trigger for chargebacks, which includes unsatisfactory experiences, failure to cancel a reservation, or simply not recognising the charge. In many cases, these disputes stem from a lack of proper

communication, unclear processes, or the unwillingness of customers to work with the hotel to resolve their issues. Although some of these chargeback requests can be legitimate, the chances of “friendly fraud” – where customers have dishonest

intentions – are also high. In fact, [nearly 75% of the chargeback disputes are “friendly frauds”](#) where customers knowingly dispute legitimate purchases, forcing hotels to bear the costs.



Authorisation issues

Incorrect transaction authorisation, where hotels fail to properly authorise a card or neglect to verify whether the cardholder has sufficient funds, can also trigger a chargeback dispute. Proper employee training and an enhanced verification process are essential in preventing these mistakes and protecting your business from chargeback fraud.



Processing errors

Simple processing errors – charging a guest twice or billing them the wrong amount, are also causes of chargebacks. Mistakes like these, unintentional or malicious, can damage the hotel's reputation and lead to unnecessary financial losses. Secure and efficient payment systems are essential for chargeback prevention in such cases.



Unexpected charges and service disputes

Lastly, unexpected charges – whether for incidentals, minibar use, or service disputes – can trigger a chargeback. If the guests feel blindsided or disagree with the charges, they may feel compelled to opt for chargeback rather than resolving the issue directly with the hotel. Transparent billing processes and policies are essential to maintain customer trust and avoid disputes for chargeback prevention.



By recognising these common causes, hotels can adopt targeted measures to mitigate chargebacks and reduce the likelihood of costly chargeback fraud.

The impact of chargeback fraud in the travel and hospitality industry

Designed to be a protection measure, chargeback allows customers to dispute a transaction, where the banks then withdraw and hold the funds from the merchant's account during dispute resolution. In the hotel industry, it can

have serious financial and operational consequences – including temporary revenue loss, additional fees, and waste of time and resources necessary to navigate the lengthy resolution process. With the instances of chargeback frauds growing

– with the travel and hospitality industry facing [a \\$25 billion chargeback volume in 2023](#) – the need for effective chargeback fraud protection strategies becomes paramount to protect both profitability and customer trust.

Strategies for chargeback prevention

Chargeback fraud protection requires a multi-layered approach that combines technology, employee awareness, and customer-facing strategies. Here are seven key strategies that can help the travel and hospitality industry reduce the risk of chargebacks:



Strengthening payment verification processes

A robust payment verification system is often the first line of defence against chargeback fraud. Implementing an enhanced verification process, including using address verification services and card verification codes, ensures the cardholder's details match the information on file. This can help detect and prevent fraudulent transactions, protecting the hotel against criminal fraud and limiting the likelihood of chargebacks resulting from unauthorised card use.



Tailored recommendations and amenities

A secure payment system is another crucial layer of protection for customers and hotels, combating the threats of identity theft, account takeover, or data breach. Tokenisation and encryption technologies can help hotels protect sensitive credit card information by replacing actual credit card numbers with tokens that are useless to cybercriminals, greatly reducing the risk of data breaches and subsequent chargeback fraud. Additionally, implementing secure online payment systems (Verified by Visa or Mastercard Secure Code) adds an extra layer of protection by requiring customers to authenticate their identity during transactions.



Implementing advanced fraud detection tools

Leveraging chargeback fraud detection software that integrates AI, ML, and behavioural analytics tools can significantly enhance a hotel's ability to identify suspicious transactions in real time. These tools can analyse patterns in transaction behaviour, flagging anomalies that may indicate fraud and abet chargeback prevention. Automated fraud detection tools can also assess risk levels for transactions, reducing manual workload while improving accuracy. Combining these technologies with two-factor authentication adds another protective layer, ensuring approval only for legitimate transactions.



Empowering employees through training

One of the most overlooked aspects of chargeback prevention is employee training. Lapses at the front desk are often major contributors to chargeback fraud. Equipping the staff with the knowledge necessary to identify potentially

fraudulent activities and how to process payments correctly – including ensuring proper identity verification, transaction authorisation, and refund management – is critical. Well-trained employees can often be a strong defence when it comes

to chargeback fraud protection, being vigilant about data security, resolving customer complaints, and preventing them from escalating into costly chargebacks.



Enhancing customer communication and transparency

Clear and accessible billing and cancellation policies are key to not only reducing chargeback disputes but also safeguarding the hotels in case of familiar fraud. Hotels should ensure that customers can easily find information about charges, refund policies, and terms of service, as misunderstandings about unexpected charges or unclear cancellation rules are common triggers for chargeback fraud. By communicating policies clearly and being proactive in resolving complaints, hotels can minimise the risk of disputes reaching the chargeback stage.



Updating fraud prevention strategies with AI and ML

As fraudsters evolve their tactics with evolving technology, the hospitality industry must also adapt its approach to chargeback prevention. AI-powered fraud prevention strategies, including the use of natural language processing and behavioural analytics, offer a more dynamic response to emerging threats. These technologies allow hotels to monitor real-time transaction data, identify unusual patterns, and prevent fraudulent transactions before they happen. This proactive approach can help significantly reduce chargeback fraud.



Collaborating for shared intelligence

Finally, industry-wide collaboration can be an important tool in the fight against chargeback fraud. Collaborative information sharing between hotels, other hospitality businesses, financial institutions, and credit card issuers can help share insights about emerging fraud trends, identify compromised cards, and prevent fraudulent transactions. Sharing insights and intelligence can ultimately strengthen the entire industry's defences.

These strategies can help the hotel industry not only reduce their vulnerability to chargeback fraud but also improve customer satisfaction and safeguard their financial health.

Conclusion

As the issue of chargeback fraud continues to plague the travel and hospitality industry, more advanced, proactive measures have become imperative for effective [chargeback fraud protection](#). Cutting-edge fraud detection tools, robust verification processes, and secure payment systems can help hotels significantly

reduce their vulnerability to fraudulent activity. Empowering employees through training and improving transparency with customers are also crucial steps in minimising disputes and ensuring customer satisfaction. With industry-wide collaboration and the integration of AI-driven chargeback

prevention strategies, hotels can effectively safeguard their operations, reduce financial losses, and enhance both security and customer trust in an increasingly digital world.

For more information, contact infosysbpm@infosys.com

Infosys[®]
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.