Sertifi

Advanced Fraud Tools

Prevent online payment fraud before it happens at your hotel

The Current Challenge

Fraudsters are committing online payment fraud through third-party bookings and same-day bookings. The fraudster will book a room using a stolen credit card, stay at the hotel, and check out before the cardholder is even aware that their card number has been stolen. Once the card has been charged, that's when the cardholder realizes that their number has been compromised. This leads to requesting a chargeback, which ultimately impacts the hotel's bottom line.

How Does It Help

- Help detect potential fraud before it leads to chargebacks
- Improve your hotel's bottom line
- Preserve your hotel's reputation
- Increase operational efficiency
- Enhance existing fraud prevention methods

How Sertifi Advanced Fraud Tools Works

1

User Fills Out Credit Card Authorization Form

Advanced Fraud Tools begin assessing data when the user is filling out the authorization form.

2

Data Assessed on the Back End

Data points are assessed to determine if a transaction has potential signs of fraud.

3

Fraud Score Displayed

Sertifi provides a risk analysis score (A-F) based on different variables.

4

You Decide How to Proceed

After a risk analysis score is displayed, you can decide whether to proceed with transaction.

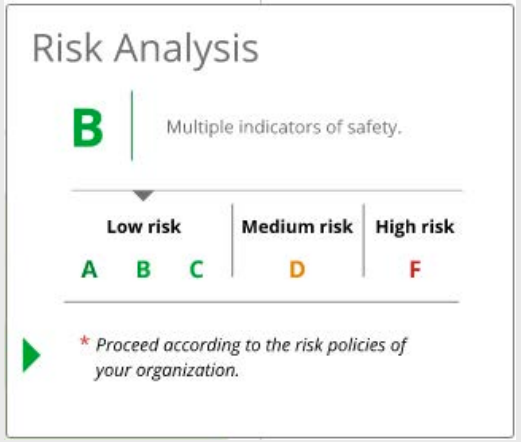
What Data is Being Assessed

- Billing Address
- Card Details
- IP Address
- Physical Address
- User Device
- Payment Type (such as the credit card)
- Email
- Name
- Authorization Status (approved/not approved)
- Country/Currency
- Payment Token
- Last 4 digits of card number
- And much more

Risk Analysis Scores - Low Risk

If the risk analysis score is an **A, B, or C**, then it's safe to proceed with a transaction.

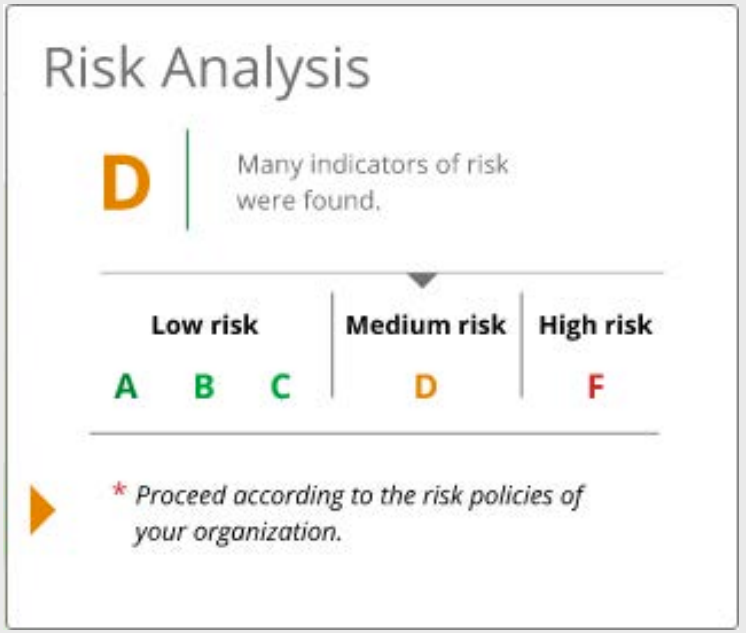
Always check your organization's policies regarding payment fraud.



Risk Analysis Score - Medium Risk

If the risk analysis score is a **D**, then it's still likely safe, but some risks were found.

Always check your organization's policies regarding payment fraud.



Risk Analysis Scores - High Risk

The riskiest transactions are the ones with an **F**.

Always check your organization's policies regarding payment fraud.

Indicators of High Risk Transactions

- IP address and Billing address are in different regions
- Physical address and Billing address are in different regions
- Previous Chargebacks associated with this user and cardholder information
- When was the email address created?
- Receiving multiple and/or simultaneous transactions from the same IP address
- Incorrect address, such as the wrong zip code
- Failed CVV verification
- Failed AVS verification