Sertifi Advanced Fraud Tools – General FAQ

Q: What is Sertifi Advanced Fraud Tools?

Advanced Fraud Tools help prevent online payment fraud before it happens at your hotel.

It puts the power back in hotel teams' hands to protect themselves against online payment fraud. Advanced Fraud Tools provides an additional layer of defense that can prevent hotels from accepting transactions that may lead to chargebacks.

Q: How much does it cost?

Advanced Fraud Tools is included at no additional charge in your Sertifi eAuthorizations subscription.

Q: Is it only available with Sertifi eAuthorizations?

Yes, it's only available with Sertifi eAuthorizations at this time.

Q: How does Sertifi Advanced Fraud Tools work?

Advanced Fraud Tools start working when a user is filling out the credit card authorization form. Using a combination of AI and data analysis, the tools use data from both the user and the card to assess if a transaction is fraudulent. The hotel staff member receives a risk analysis score based on different variables. They can choose whether or not to proceed with a transaction.

Q: What kind of data is being assessed?

The following key data points are used to perform a risk analysis.

- Authorization Status (approved/not approved)
- Country/Currency
- Email
- Billing Address
- Name
- Card Details
- IP Address
- Physical Address
- User Device
- Payment Type (such as the credit card)

- Payment Token
- Last 4 digits of card number
- And much more

Q: Why do I need Sertifi Advanced Fraud Tools?

Advanced Fraud Tools puts the power back in hotel teams' hands to protect themselves against fraudulent activity, particularly around third-party bookings and same-day bookings. Using a combination of AI and risk analysis, every transaction is assessed for potential signs of fraud enabling you to decide whether to accept a transaction. By having Advanced Fraud Tools, you're adding an additional layer of defense to your hotel that protects them from accepting transactions with chargeback potential.

Q: What problem(s) does it solve?

Fraudsters are committing online payment fraud using credit card authorization forms for third-party reservations and same-day bookings. Typically, with third-party reservations, the person paying for the room isn't necessarily the one staying at the hotel. This makes it difficult for hotel staff to validate the credit card because this is the norm in both corporate and event travel. This gap makes it easy for fraudsters to book a room using a stolen credit card, stay at the hotel, and check out before the cardholder is even aware that this happened. Once the fraudster leaves, and the card has been charged, the cardholder realizes their card number had been stolen, so they'll request a chargeback. Chargebacks impact the hotel's bottom line and reputation.

Q: Does it prevent chargebacks?

No, it doesn't guarantee there won't be any chargebacks, but it's an additional layer of defense that can prevent hotels from accepting transactions that may lead to chargebacks. Advanced Fraud Tools combined with features such as AVS and CVV help hotels to protect themselves against chargebacks. We provide the data so that hotels can decide whether to proceed with a transaction.

Keep in mind that no one product can truly prevent chargebacks. It requires a multi-layered approach to protect your hotel from online payment fraud and chargebacks.

Q: Will there be any type of training?

Visit the Sertifi Support Center for Advanced Fraud Tools training material to help you get started. If you have any issues, you can submit a ticket to support_ticket@sertifi.com.

We will have a webinar that offers guidance on when to proceed with transactions in the future. These best practices will be based on data that we've evaluated, however, it's ultimately up to the hotel to decide whether to proceed with a transaction.

Q: Why does Sertifi need to assess all that data?

Sertifi has determined that there are many different variables that indicate potential online payment fraud activity. This data is needed to perform a comprehensive risk analysis on each transaction so that hotel teams can make an informed decision before proceeding with a transaction.