

# FRAUD OVERVIEW: CARD TESTING

In addition to fraudsters booking hotel rooms with stolen credentials, hotel brands are also the target of payment card testing schemes. As a result, hotels suffer from lost revenues, poor customer experience and excess inventory from held rooms.

## STEP 1

SCAMMER TESTING STOLEN CREDIT CARD NUMBERS ON A HOTEL OR BRAND WEBSITE IS ABLE TO GET A PRE-AUTHORIZATION TO KNOW THE CARD NUMBER IS STILL VALID.



Frequent hotel reservations come from a common browser signature/cookie/device using many different card numbers.

## STEP 2

THE RESERVATION IS NOT CANCELLED AND A LEGITIMATE CUSTOMER IS CHARGED A CANCELLATION FEE OR A FULL FEE



Loyalty programs often have less stringent fraud measures in place.

## STEP 3

CUSTOMER INITIATES A DISPUTE AND THE HOTEL SUFFERS FROM LOST INVENTORY/REVENUE, TIME AND EFFORT TO HANDLE THE DISPUTE



Cardholder disputes fee and charge is reversed.

# IDENTIFYING HIGH RISK ACTIVITIES (RISK ASSESSMENT)

## ACTIVITY DETAIL

## RISK ASSESSMENT (HIGH, MEDIUM, LOW, ETC.)

### MONITOR IP/DEVICE VELOCITY

Establish velocity checks for browser signatures/cookies/devices/email addresses and BIN

HIGH - when many reservations (including failed attempts) come from a single device, account or IP address.

# PREVENTION TECHNIQUES & PROCESSES

## INSTRUCTIONS

## DEPENDENCIES & DETAILS

### ESTABLISH RULES AND MONITOR VELOCITY FOR BOOKINGS

Create rules that will block browser signatures/cookies/devices/emails that appear to be associated with card testing

Link search will enable hotels to identify related orders

### MONITOR BOOKING SITE FOR BOT ATTACKS/AUTOMATED TRAFFIC

Partner with IT teams to implement solutions to identify and deflect robotic or automated traffic

Partner with your technology team to identify BOT/scripted traffic via site navigation analytics