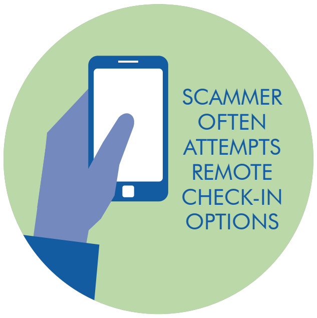
FRAUD OVERVIEW: CREDIT CARD AUTHORIZATION FORM

Since transitioning to chip-enabled card readers and with heightened awareness around remote check-in methods for same-day bookings, fraudsters have reverted to an old scheme – using fraudulent credit card data on Credit Card Authorization Forms. Credit Card Authorization Forms are difficult to validate when received at check-in (or shortly before), making them an attractive method for fraudsters to obtain room keys.

Most hotels do not validate a comparison of name/address from the booking details to the card details.

Last minute bookings are less likely to be researched by the hotel prior to arrival.



Remote check-ins remove the face-to-face encounter with hotel staff.

Pre-filled and signed authorization form is provided at check-in which gives a clerk no time to validate the card information prior to releasing room keys.

IDENTIFYING HIGH-RISK ACTIVITIES *(RISK ASSESSMENT)*

	ACTIVITY DETAIL	RISK ASSESSMENT (HIGH, MEDIUM, LOW, ETC.)
LAST MINUTE CREDIT CARD AUTHORIZATION	Guest provides pre-filled and signed form in person at check-in	Always HIGH-RISK! Recommended to not take forms after 72 hours prior to check-in
SHORT NOTICE CREDIT CARD AUTHORIZATION	Guest books online for immediate arrival	MEDIUM on its own HIGH in combination with others Recommended to not take forms after 72 hours prior to check-in
SAME DAY BOOKING	Guest attempts remote check-in methods	MEDIUM on its own HIGH in combination with others
CHIP FAILURE	Guest reader shows card is chip-equipped but card has no chip or card reader, showing CHIP FAILURE	Always HIGH-RISK!
CHECK-IN METHOD	Guest attempts remote check-in methods	HIGH in combination with others

PREVENTION TECHNIQUES & PROCESSES

	INSTRUCTIONS	DEPENDENCIES & DETAILS
72-HOUR WINDOW ON CREDIT CARD AUTHORIZATION FORMS	A physical card must be present and should be inserted, swiped or tapped at the time of check-in to secure for incidentals	Do not accept credit card authorizations on same-day and high-risk bookings.
CHANGE LANGUAGE ON CREDIT CARD AUTHORIZATION FORMS	Announce the 72-hour window Announce card can be billed as soon as immediately after receipt of form	By providing written notice that you will not accept the form within a 72-hour window prior to arrival and of your intent to bill the card as soon as the form is received, you can protect your revenue from declined authentications AND fraud holds on the card you have received. This also aids the front desk to have policies in place that they can cover with the guest upon arrival.
FACE-TO-FACE CHECK-INS	Force a face-to-face encounter	Disable all remote check-in options for high-risk bookings. Perform a welcome check at the room or flag the room number to have a manager greet the guest in the dining room.
VERIFY IDENTIFICATION	Request the guest presents photo ID (note that in cases of fraud, the checking of ID doesn't provide any protection for the hotel)	Verify that the name on the ID matches the guest name, and ensure the name and address are attached to the reservation. Note: This can assist in cases that escalate to involve investigation by local authorities.
VERIFY PHYSICAL CARD	Request the guest to present the payment card	Verify the name on the card matches the guest name, and that it is the same as the booking payment method. Verify that the last 4 digits of the physical card match what is reported when the card is swiped/chipped into the POS.
DO NOT ATTEMPT MANUAL AUTHORIZATIONS	A valid electronic authorization must be obtained in order to release room keys to the guest	If the guest's card is declined by the system, insist on a new method of payment. Once a decline is received, ask the guest for another form of payment. Do not attempt voice authorization, manual or forced authorizations; do not allow the guest to "call their bank" for an authorization. If the guest presents a large number of declined cards, you are within your rights to request cash-only payment at check-in.