FRAUD OVERVIEW: LOYALTY ACCOUNT TAKEOVER FRAUD

In addition to fraudsters booking hotel rooms with stolen credentials, hotel brands are also the target of account takeover. As a result, hotels suffer from lost revenues, poor customer experience aexcess inventory from held rooms.

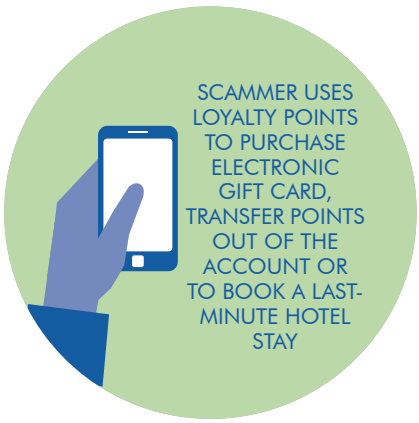
STEP 1

Hotel loyalty programs are often managed by a third party or within a different business unit than the payment fraud group. As a result, fraud screening may be less robust.

STEP 2

Loyalty programs often have less stringent fraud measure in place.

STEP 3



Scammer may change e-mail confirmation/contact details on loyalty account prior to perpetrating fraud.

IDENTIFYING HIGH-RISK ACTIVITIES *(RISK ASSESSMENT)*

	ACTIVITY DETAIL	RISK ASSESSMENT (HIGH, MEDIUM, LOW, ETC.)
CHANGES TO ACCOUNT INFORMATION PRIOR TO A REDEMPTION ACTIVITY	Account details are changed prior to a redemption or points transfer	HIGH in combination with others
LAST-MINUTE BOOKING FROM A REGISTERED ACCOUNT	Last minute booking using a card on file	HIGH in combination of IP mismatch and the name of the account does not match the ID of the person checking in
GIFT CARD REDEMPTION	Points are redeemed for gift cards	HIGH in combination with others
IP ADDRESS MISMATCH	IP address from device does not match one in customer profile	MEDIUM

PREVENTION TECHNIQUES & PROCESSES

	INSTRUCTIONS	DEPENDENCIES & DETAILS
DEPLOY DEVICE AND USER BEHAVIORAL ANALYTICS JAVASCRIPT/SDK	Collect device attributes and User Behavioral Analytics for all login activity	Build a customer profile of associated devices/IP addresses and typical behavior.
	Monitor and incorporate login activities to transactions (e.g. did the individual change the e-mail address and then transfer points?)	Monitor anomalies. If out of pattern behavior - consider using more data to assess the risk and/or step up authentication prior to completing a transaction.
VELOCITY RULES	Track and incorporate velocity rules into fraud scoring assessment - IP, e-mail, mobile, device ID	Understand typical and atypical velocities for key fraud attributes and monitor for out of pattern trends.
VERIFY ID AND NAME ON FILE	For last-minute bookings, confirm the name on the account matches the name of the guest checking in	Train associates to use a multi-point identity check.
SINGLE FRAUD STRATEGY ACROSS REWARDS AND PAYMENT PLATFORM	Have a consistent approach to managing fraud across payment and reward platforms	Ensure learning and data is shared and managed consistently across payment and reward programs. Require separate confirmation of account changes via email, text message, or other channel prior to allowing transactions against the account. If the transaction looks suspicious, require a credit card to complete the loyalty transaction. If the card on file is used, require the CRC or verification code on the card to complete.