PROFiT
Prevention of Fraud in Travel

# THE COUNTER FRAUD CAMPAIGN 2019

## PART 9: VALIDATING A BOOKING

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. In PART 9 we begin to look at payment crime issues.

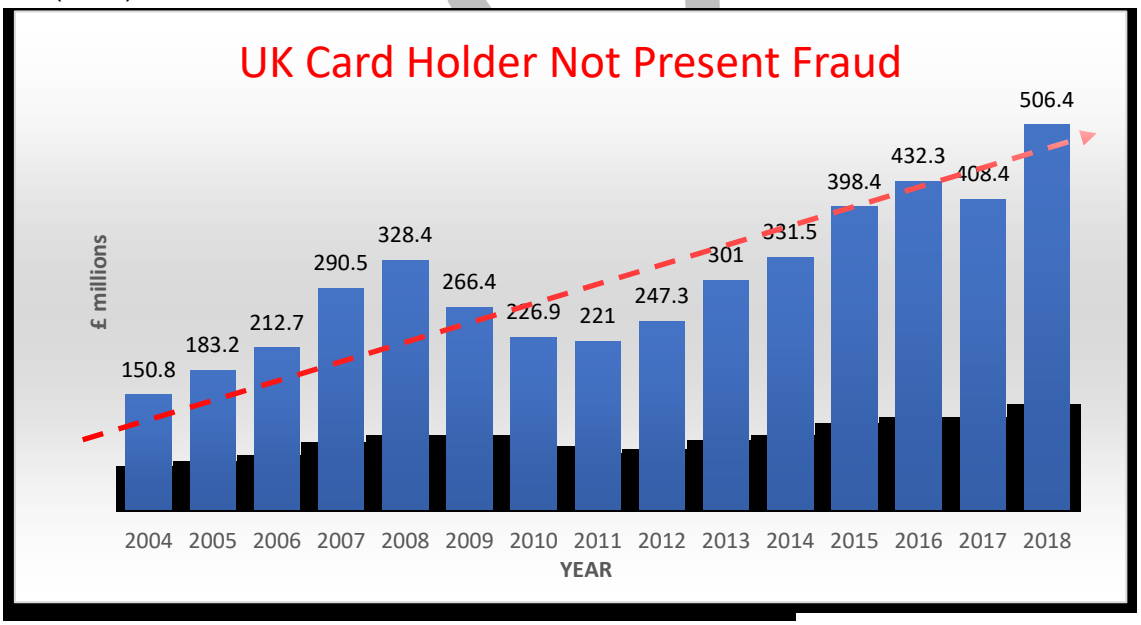
PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

**Find out how you can join the fight against crime. Contact via:** contactus@profit.uk.com

### BACKGROUND

1.0 The most common method of paying for travel arrangements is through payment cards especially with the move to online and mobile purchases of goods and services. When the correct processes are in place a payment card is a safe, secure, and convenient substitute for a cash transaction.

1.1 Payment fraud is the the form of crime most visible to a company and where much effort and money is expended trying to reduce the risks. Banking industry figures show that Card Holder Not Present fraud has increased by over **230%** since 2004 from £150.8 million to £506.4 million in 2018. The trend looks set to continue into the foreseeable future. This rise has occurred despite the proliferation of verification tools, the introduction of security measures such as the Card Security Code (CSC, also identified as CVD or CVV) in 1997, and Chip and Pin (CNP) in 2006.




**SOURCE:** UK Payments

### HOW DO PAYMENT CARDS WORK?

2.0 When a payment card is swiped or keyed a transaction for the payment is generated. Upon approval of the sale, a receipt is given to the customer. For swiped, face-to-face, transactions in the UK the customer usually enters their PIN number into a secure encrypted pad, or in a limited number of cases signs a copy of the receipt usually when the terminal is unavailable.

2.1 In the case of contactless payment pads there is no validation after the card is swiped. Call centre transactions require the seller to enter the card details into their payment terminal. Online transactions require the customer to enter their card details and security code into a template which acts as a substitute for a payment terminal. The transaction takes place once the seller's equipment connects to the payment network and usually only takes 3-4 seconds.

2.2 However the payment is initiated the sales information travels from the processing equipment across the secure payment network to where the seller's 'merchant account' is located and an authorisation request is created and sent to the customer's bank where the card was issued. The customer's bank receives the request. If the customer used Chip and PIN then the transaction is already authorised but if Chip and PIN is not used the customer's bank performs a series of tests to make sure there is enough credit available to cover the sales amount.

2.3 The authorisation request is either approved, if funds are sufficient, or declined. A response is sent back to the merchant account, where the transaction is added to a payment batch and then sent back to the originating seller's processing equipment. If the authorisation request is approved, the customer's bank secures funds for the payment.

2.4 All transactions go through a settlement process. This process is initiated by the seller closing their open payment batches which are normally processed at the close of business each day. During the settlement process the funds are moved from the customer's bank into the seller's 'merchant account', and then deposited into the seller's business bank account. Depending upon the contract the seller has with the card acquirer it can take varying amounts of time to settle a payment batch but typically it takes several days. Generally, debit card funds are transferred quicker than credit card funds due to the different networks and processes involved.

## PROBLEMS WITH CARD PAYMENTS

3.0 Either through misuse, theft or personation, several payment card transactions will present problems for retailers. Generally, merchants face greater difficulties identifying criminal card use when taking remote transactions than they do with face-to-face transactions. A misused, or fraudulently used, card is likely to result in a chargeback to the merchant. Where the card acquirer identifies a high number of chargebacks they may pass on a fine to the merchant from the Visa or Mastercard scheme as appropriate.

## WHY ORGANISATIONS NEED TO VALIDATE A BOOKING

4.0 Where transactions present a problem to the retailer then a manual review will be necessary in order to ascertain if the booking should be accepted or rejected. Whether taking online or 'Call Centre' bookings there are a few simple steps you can take to assist you in making your transactional decision a safer one.

<u>Review the details of the booking</u>

4.1 Depending on how the booking was made you should have access to some or all of the following pieces of location information.

- **IP Address** - Compare the IP address location to the other location details given by the potential customer; the IP Address, bank account, and physical address which should match.
- **BIN** (Bank Identification Number) – A BIN is the first 6 digits stated on a credit card from the 16-digit number. The BIN identifies where the credit originates from, what bank the credit card is from and the type of card. If a customer has provided information that suggests they are based in the UK by checking the BIN you can establish if the origins of the credit card match the other details the customer has provided.
- **Email address** – Make use of social media to see if you can find the email address in use, look at the history of the user to help you make a decision about the booking.

4.2 Where a customer gives a UK address, an overseas located payment card, but the IP address is showing an entirely different location to both of these location data then the transaction is highly

risky and further checks should be made before proceeding. For a list of free tools to assist you with validating a booking visit: www.profit.uk.com/free-fraud-prevention-tools

**Speak to the lead passenger**

4.3 During the booking process you will probably collect at least three pieces of information that will enable you to contact the lead passenger of a booking, namely a postal address, an email address and a telephone number. Experience shows that where a fraudulent booking has taken place you are often unable to contact the stated lead passenger; if you are checking a booking and are unable to contact the lead passenger you have good reason to reject the booking.

4.4 Before rejecting a booking it makes sense to take every possible step to contact the lead passenger in case there is a legitimate reason for their shyness. The amount of time you allow the customer to come back to you will be dependent on when the travel arrangements commence and when costs will be incurred by your business for the services purchased.

4.5 Where you can speak to the lead passenger then the following steps should help you ascertain that the booking is genuine:

4.5.1 Confirming the details given during the booking process

Ask the lead passenger to confirm details of the booking made. A genuine customer should, without being told by you, have no problem confirming the personal details given, while a fraudster may not have such information to hand so may be more hesitant in supplying such information.

4.5.2 Ask questions about the data given

A clever fraudster may well have all the personal information relating to the booking to hand so to confirm they are who they say they are you may choose to ask a question based on the information they have given. This may include asking them a question about where they live like a street name near their home address, or a building of significance in the area of residence. You will be able to use Google maps or a similar street mapping system to find these matters out. Other questions that could be asked could include who else lives at the postal address stated or what type of payment card was used for the transaction?

4.5.3 Proof of Identity

If all else fails, you can ask them to send a copy of their identity document over so that you can verify it visually.

Nothing is infallible, but by being creative you can validate bookings to reduce the risks of payment fraud.

**Next Week: Part 10 Payment Fraud Issues**