PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 10: PAYMENT FRAUD ISSUES

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 10 we identify how and why payment fraud occurs.

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 Every retail organisation faces the prospect of being defrauded though its payment mechanism. Payment fraud is perhaps the crime most businesses focus upon. Not only is it highly visible; it adversely affects the company's income and may lead to banking penalties. Despite the effort companies expend to secure payments criminals still manage to exploit the situation in order to commit fraud.

1.1 This issue of the email campaign looks at some of the factors which mean that, despite paying for 3rd party solutions, following banking and consultant advice, and having good systems, companies can still fall victim of online payment fraud.

SOME THINGS YOU SHOULD BE AWARE OF:

ISSUES RELATING TO CRIMINALS

2.0 A proportion of your failed payment attempts will be made by organised crime. Criminals test out company systems by making multiple purchase attempts, this gives them insight into the systems and processes companies use. Often these attempts are carried out on a massive scale against several companies at once by 'Internet Bots.'

2.1 An internet bot is a software application that runs automated tasks (scripts) over the Internet. Typically, internet bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. In your normal life you will find chatbots on many messaging apps, including Facebook Messenger, WhatsApp, and Telegram. Even the more work-focused service Slack has its own built-in bot that helps you set reminders and jot down notes. Twitter has bots too which will reply to you, but usually not offer any assistance.

2.2 When the criminals use internet bots, they do so in order to test your companies' systems, and processes which they may share with other criminals online because they know that alert companies may identify that they have been targeted and so the window of opportunity may be short. By sharing the compromised data on company anti-fraud measures, criminals maximise their own opportunities.

2.3 Organised criminals know that the best time to facilitate payment fraud against a travel company is when there is less likely to be anyone working that might scrutinise transactions. PROFiT case studies continually demonstrate that a disproportionate number of fraudulent travel transactions occur out of office and call centre working hours.

ISSUES RELATING TO VALIDATION TOOLS

2.4 PROFiT strongly recommends that every organisation should use third party tools to validate the lead passenger and/or the payment/person making the payment but be aware of their weaknesses.

2.5 All organisations should be mindful that many of the 3rd party validation tools are not working with live data, nor do the branded tools operate in the same manner as each other. Some 3rd party tools make exaggerated claims about their efficacy and data sources that they use.

2.6 The most popular method of operation for validation tools is to rely upon 3rd party data. This can be broken down into:

- '**Broad data systems**' which look at a few details across a broad range of data sources. Typically, the systems look for, as an example, a person's name within data lists such as births, deaths and marriages; electoral rolls; politically exposed persons; etc. They validate the name by identifying it in a number of these 3rd party lists. Unfortunately for the users they often work on data of unknown age, quality, and provenance.
- '**Narrow data systems**' which look at a small number of details against a narrow data set. Typically, the data set used is live or regularly update data. Using our example of a name, the validation tool looks to see how many times the name has appeared along with the address searched for within a single set of data. In this way these systems can give a high degree of confidence if the name appears against that address very regularly. For example, the validation tool may check whether a person's name has appeared against live financial data and identify that the name being searched for has been involved in a loan, a mortgage and numerous bank transactions at the search address over a long period of time.
- '**Data cache systems**' look at a pool of cached data, usually supplied by the users of the system themselves. Where these types of tool have clearly defined rules and procedures for adding, searching and using the data they can be effective, but many systems do not define what types of data can be entered sufficiently tightly and may have questionable operating systems.

2.7 Some validation tools interfere with the operation of other validation tools when used in conjunction with each other, so care needs to be taken when selecting more than one system and using them simultaneously.There are no validation tools currently on the market that indicate when unsuccessful attempts to transact occur, therefore they do not let you know when criminals are testing your systems.

2.8 Validation tools only check the lead passenger and the payment. Where the payment is made with a compromised card that has not yet been reported then they will be accepted as valid by all validation tools. You should also be aware that career criminals know that if they put their name first on the list of travellers, they will be checked and probably discovered so they will generally be further down the group listing of passengers and ignored by validation tools.

ISSUES RELATING TO BANKING

2.9 Every payment case study that PROFiT has undertaken shows that a high proportion of payment fraud occurs within 7 days of departure. When a person's payment card is compromised the details are circulated on the VISA TC40 or Mastercard SAFE report, but this does not generally occur less than 10 and 14 days after the payment card has been identified as compromised. Therefore, these reports will often fail to prevent fraudulent travel bookings.

2.10 A fraud unique to travel occurs where a group of perhaps six people travel and one person pays for the group on their payment card but then, once they have returned home, falsely claims that that their payment card had been compromised as they have no knowledge of the group travel and they make a chargeback. Each person in the group does the same thing on

subsequent trips such that for six trips the group has free travel. The group of fraudsters are all viewed individually by their respective card acquirers and as they are 'clean skins' their chargeback is accepted, and this is not recognised as a fraud by the banking system.

2.11 Be aware that when you employ a bank or acquirer anti-fraud system, they are often configured for the UK market and so reject non-chip and pin transactions. Unfortunately, the travel industry operates in regions of the World where chip and pin has not yet been implemented. This means that genuine valuable bookings will be lost if you are not aware of this take remedial action to independently validate these 'lost bookings.'

ISSUES RELATING TO COMPANY SYSTEMS

2.12 Organisations need to make sure that the whole of their systems for taking payments are secured and the risk of staff being able to make rogue bookings without putting them through the company systems is minimised.

2.13 PROFiT has investigated a number of cases where homeworkers have taken 'bookings' in the company name and either paid them into a bank account that they have set up with a similar name to the company, or alternatively, they have taken payment in cash or by money transfer and not put this through the company systems. However, such activity is not confined to homeworkers and organisations should be aware that any person in the transaction chain is capable of this type of deception from sales staff up to the most senior financial supervisors and managers.

2.14 The latest trends in payment fraud also undermine the efforts of company's payment fraud solutions. During 2019 there has been a rise in staff members that whilst still working for their employer set up social media pages using the employer's branding and purport to sell travel arrangements in the employer's name, when in fact the bookings are bogus which avoid company systems.

2.15 These bogus 'bookings' by-pass the company systems and payment mechanisms but are made in the company name and so eventually the victim approaches the company demanding to know where their travel arrangements are. The company has no records of any such bookings and is unable to deal with the victims.

MISSED A PREVIOUS EDITION?

If you have missed a previous edition of the email campaign let us know and we can send you FREE a copy: contactus@profit.uk.com

1. Fraud Risks
2. Recruitment in Travel Fraud
3. Employee Fraud
4. Your Supply Fraud
5. Upon Discovering A Fraud
6. Investigating A Fraud
7. When Police Become Involved
8. Preparing For Court
9. Validating A Booking
10. Payment Fraud Issues

Future editions will deal with brand protection and cyber crime.

Like what we do? We always need support. Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com.

Next Week: Part 11 Challenging A Chargeback