PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 12: OTHER PAYMENT FRAUD

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 12 we look at other methods that criminals use to divert company funds into their own accounts.

against the organisation.

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

BRAND APPROPRIATION

WEBSITES

1.0 For several years it has been possible for criminally minded people to clone a travel website in its entirety, change the contact details to their own, and then published the cloned website under a domain name similar to the legitimate site that they have copied in order to attract victims.

1.1 Using copying technology cloning a website only takes a few minutes to do. Often these sites are almost identical to the genuine website such that the legitimate owner of the cloned site finds it hard to spot the scam.

1.2 Many cloned sites can readily be identified by careful inspection of the domain name, also known as the Universal Source Locator (URL), which may vary from the original by missing out a letter, adding a letter, or inserting a symbol such as a full stop or hyphen into the text. They also tend to lack of functionality of the tabs and buttons. The most sophisticated cloned sites will replicate the victim website exactly in all aspects and can only be identified by the contact details and scrutiny of the domain name.

1.3 From a criminal's perspective copying the coding of a company's website has a drawback as it only permits the criminal to use it to commit a scam in the persona of that one company.

1.4 A second type of bogus website occurs where the criminal builds a basic website and 'skins' it to make it look like a genuine site. Due to the short life of this type of site the scammers only concern themselves with limited functionality.

1.5 With this type of clone, it is common for some tabs and buttons to be inoperative. Another clue is that, where they can be bothered to have them at all, they will copy terms and conditions from a genuine website but not bother to change these when they 're-skin' the site so an easy clue that the site is bogus will be references to a completely different company in the terms and conditions and, where it exists, privacy statement.

1.6 The way that this basic type of 're-skinned' website is configured chameleon-like means that it can easily be used time and again as it does not take long to change the look of the website. In changing its identity, it may appear as another company's travel website, or a unique website made

up by the criminals very quickly.

1.7 All cloned websites trade by stealing a legitimate company's customers. The most common way for the criminals to steal customers is to bid on the company's brand terms in Google to gain maximum visibility to potential victims. To obtain live offers cloned websites often 'scrape' the target websites offers. Since cloned websites don't intend to fulfil offers, they can only operate for a short period of time once they begin to scam customers before they must rebrand themselves.

1.8 In the past it was relatively easy to identify who was behind a website and to contact the registrar, provide evidence, follow the disputes procedure and the registrar removed the website. It has become much harder to get cloned websites removed nowadays as criminals hide behind privacy policies and registers make it harder to remove bogus domains.

SOCIAL MEDIA

1.9 Recently criminals have become more prominent trading as travel companies on social media platforms. Often these social media pages trade using their own bogus company names but increasingly they use copies of actual travel company's social media branding.

1.10 Several times it has been identified that the bogus social media copies of a company's branding have been set up by the company's own employed staff. It appears that the staff set up a social media page that uses the branding of their employer and which they use to surreptitiously trade alongside their legitimate employment. So far as consumers are concerned the social media page is indistinguishable from the company itself even though it is unauthorised.

1.11 Whilst the staff committing this type of fraud are fulfilling your offers they are also trading outside of your systems and providing bogus paperwork modelled on your own branding which makes this crime very difficult to discover until the victims make contact to complain. The motivation for this type of scam is often the need to fund lifestyle, debt repayment, or addiction.

1.12 All company employees carry out their duties on a trust basis. Company systems back up the trust inherent in the contract between the parties but no matter how good your systems are there will be some scope for anyone with access to the payment journey to divert funds into their own bank accounts.

1.13 Social Media platforms have not been set up to facilitate trading and most do not have any policies for removing bogus travel pages that are reported to them. The most popular social media platforms for bogus trading as travel companies are Facebook, Twitter, Whats App, Messenger, Snap Chat, Instagram, Tumblr, Tik Tok, Reddit, Pinterest, and LinkedIn (usually business travel related). It is very difficult to get any page carrying out criminal activity removed.

1.14 We will look at what you can do to improve you chances of removing bogus websites and social media pages in the 14th email campaign release.

PAYMENT DIVERSION

2.0 There are various ways criminals external to the organization can divert company funds, usually in the form of payments that purport to be due to a 3rd party. The simplest way to achieve payment diversion is to just contact the finance team and persuade them that a payment is due.

BOGUS INVOICES

2.1 A common criminal tactic against all businesses is to send in a bogus invoice for payment to the finance team of a travel company. The false invoice may be from a phony supplier, it may purport to be for a non-existent advertising deal, or a fake trademark renewal or a host of other ingenious but simple scam reasons. Often the convincing invoice will be planned to arrive during a holiday period when it is likely that less experienced staff are processing payments and anyone that they need to check the invoice with is away.

2.2 This bogus invoice fraud is relatively simple to combat; introducing a policy that invoices will only

be paid where there is a pre-existing order in the system prevents bogus invoices being paid. To further secure your company funds you could insist that invoices refer to the order number and carry the name of the staff member that raised the order. Adding simple requirements such as these makes it harder for a fraudster with little knowledge of the organisation to game the system.

2.3 The most effective, but also bureaucratic, way to defeat this type of fraud is to only deal with suppliers that are on a pre-existing list and have all been pre-registered and checked out by the company. However, this means that every time a new contract is entered into, even for the smallest of items will need to go through a time-consuming process.

BOGUS PAYMENT REQUESTS

2.4 A common criminal tactic is to send an email to the accounts payable team which appears to come from a credible senior manager such as the CEO, Head of Sales or Marketing Director. The content of the email will usually require a payment to be made quickly on some pretext.

2.5 There are a variety of ways that the criminal can glean the information required to design the spoof email such as finding out key personnel from a company prospectus, identifying staff on Linkedin or social media, or simply calling the switchboard and inquiring. Because companies persist in using an email address that is connected to their domain it is relatively easy to guess the format of email addresses added to which many people give this information away freely on social media.

2.6 This type of fraud can be completely countered by only fulfilling demands for payment where an invoice exists that relates to an order in the system. Where the demand for payment is made, an invoice and order are not in the system, and finance staff are not confident enough to just deny payment then it is easy enough for them to walk around to the alleged originators desk to confirm the intention, or to contact them using the persons phone number or email them using the details recorded in the company systems for the same purpose.

SPOOFING SUPPLIER DETAILS

2.7 A relatively common form of fraud is to contact the finance team of a travel company claiming to be a new contact of an established supplier to the company and giving new bank account details for payment. Once they have duped the travel company into changing the bank account the criminals sit back and receive the funds wrongly paid to them.

2.8 It is not clear how criminals identify which suppliers a company trades with, but one known method is to hack a supplier's own systems, identify clients which they have, and then use that to commit fraud against the whole client list. It is possible that some instances of this type of fraud are speculative as some suppliers are so big that they are likely to be used by a high proportion of the market. One further possibility which should not be discounted is that the victim company's own systems may have been compromised and when this occurs it is not uncommon for the fraudster to simply change the bank account details for payment within the company system.

INTERNAL FUND DIVERSION

2.9 The most common diversion of funds occurs internally which often does not come to light for some time, or at all, depending upon how good internal accounting systems and auditors are. Anyone in the sales or payment hierarchy, from a board member down to a home worker can divert payments due to the company. Often the crime occurs because staff see poor oversight and have developed a lifestyle or habit which requires funding.

2.10 Sometimes this type of fraud may involve simply booking clients travel arrangements in the company system as normal but taking the payment themselves. Other variations involve the criminal laying off bookings to a third party or using a compromised payment card to place the booking into the company systems whilst diverting the actual payment to themselves. Criminals undertaking this type of crime will often require payment by bank transfer or cash to prevent the victims making a chargeback against them.

2.11 Over the years research by PROFiT has shown that the perpetrators of this common type of fraud

manage to commit between £5000 and £15000 (for sales staff), and up to several millions of pounds (for more senior employees) of fraud before detection. Because travel companies do not report the crime and are reluctant to provide bad references for fear of being sued perpetrators often go on to repeat the crime multiple times before finally being stopped.

2.12 To identify this type of crime, be on the lookout for staff living beyond their means, taking multiple fancy holidays, buying property, erratic behavior, avoiding scrutiny by aggressive behavior or driving fast cars. Be aware when staff start talking about gambling habits, debt or problems at home and, where you can do so, consider putting in support as these types of issue may be precursors to committing fraud.

2.13 Making it harder to commit internal fund diversion fraud involves;
* ensuring good oversight of any staff taking bookings or processing payments and refunds;
* ensuring passwords are not shared;
* ensuring that staff who can make refunds are not the same as staff who take payments;
* rotating the staff overseeing the financial systems and processing the bookings regularly;
* only allowing access to booking systems and payment systems to those that need to use them;
* locking down key company systems so that they are harder to misuse;
* checking for discrepancies between the payment gateway and booking system; and
* checking lists of payments made for repeat instances of the same card number.

2.14 When you do identify this type of fraud you need to confront the perpetrator, carry out a thorough investigation, remove their access to company systems, and seek cooperating from the perpetrator to identify the extent of their wrongdoing. We do not recommend that you strike a deal with the criminal as we have seen many times that the criminal will only disclose what they think they can get away with and after they have gone further crime will often come to light.

2.15 We always recommend that companies report this type of crime to Action Fraud using the online reporting tool https://reporting.actionfraud.police.uk/login or by calling **0300 123 2040** Monday to Friday 8am - 8pm.

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 13 PROTECTING IMAGES