



THE COUNTER FRAUD CAMPAIGN 2019

PART 7: WHEN THE POLICE BECOME INVOLVED

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 7 we look at what you can expect when the police become involved and this edition reinforces why it is important for all organisations to take the advice contained in the PROFIT email campaign and use it to harden themselves against fraud.

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

1.0 REPORTING FRAUD

- 1.1 Reporting crime benefits you, benefits your industry, and benefits society by:
 - Protecting the public from future criminal conduct,
 - Reducing the cost to society caused by fraud and corruption,
 - Reducing the risk of a further attack on your business from the same criminal(s),
 - Enabling compensation to be paid to the victims from the recovery of funds and assets obtained as a result of the criminal activity
 - Maintaining confidence in the UK's business and financial institutions
- 1.2 The police report that you make could provide valuable information which may contribute to a successful investigating and prosecution of criminals. Many frauds that affect industry appear to be an isolated one-off event but in fact are organised by criminal groups and affect many other companies. The police rely on your information, as industry practitioners, to help them stop fraud and money laundering criminals. Everyone has a duty to report crime and it is your responsibility to do the right thing and tell the police so that they can act.
- 1.3 Regardless of anything that you read in the press or is contained in this document we recommend that you should always consider reporting crime to the police, including making fraud reports to Action Fraud, as the aggregated data is the only measure likely to obtain increased police resources to deal with fraud over the longer term.

2.0 HOW TO REPORT A FRAUD

To report fraud or cyber enabled crime in the UK use the Action Fraud website. You can report a fraud to Action Fraud by using the online fraud reporting tool <http://www.actionfraud.police.uk/home>, or by speaking to a specialist fraud adviser in the contact centre on 0300 123 2040.

- 2.1 **Action Fraud** is the police 'one-stop shop' that records National Fraud Intelligence Bureau (NFIB) fraud and some cyber-enabled and cyber-dependent crimes such as Computer Misuse Act offences like hacking. **Action Fraud** does this through its' contact centre and on-line reporting tool. With the exception of crimes meeting the 'CALL FOR SERVICE' criteria (see below) the majority of economic and cyber enabled crimes will be recorded at the NFIB directly by data providers and by victims using the '**Action Fraud**' on-line reporting tool or the **Action Fraud** contact centre.

- 2.2 Where victims contact their local police force to report a fraud, police will, unless a 'CALL FOR SERVICE' exists (see below), inform the victim that they can report fraud themselves to Action Fraud directly via the contact centre by telephone or on-line reporting tool. If this advice is taken, then the local police will not record a crime. Where victims decline this facility and ask police to record a fraud, the local force may take full details of the fraud and pass the details to NFIB.
- 2.3 When reporting a fraud via the online fraud reporting tool, you will be taken to a new website address. This is because the online fraud reporting tool has additional security on it to protect your information. You'll notice that the website address begins with 'https', which means the website, has a security certificate attached to it. When you complete the form and submit your information, it is sent to Action Fraud over a secure internet connection. The online fraud reporting tool will take you through a series of questions about the incident you are reporting, including questions about the suspect. If you need help whilst completing the form you can ask one of the online advisers by clicking on the "Online advisers, live help" button and chatting online within the tool.
- 2.4 You will normally need around 20 to 30 minutes to complete the form. Once you have started the form you will need to complete it in one session, so before you begin, make sure that you have all the relevant information to hand. For example, names, dates, information about the suspect, who is affected, and details of how any money was lost. Please make sure that you are happy with the information which you have entered on each page before continuing, as information already entered will be lost and will need to be re-entered if you return to a previous page.
- 2.5 You can also report fraud by speaking directly to a Specialist Fraud Adviser by phoning **0300 123 2040**. The advisor will also be able to give you help and advice about fraud. The fraud specialists are available from:
Monday to Friday between 8am to 9pm
Saturday between 9am to 5pm
Sunday between 9am to 5pm

You should bear in mind that it is a criminal offence to make a false report.

Obtaining Police Action When A Fraud Is Actually Happening

- 2.6 The Home Office Counting Rules require fraud to be treated like any other offence so that where the following "call for service criteria" applies the Police can be asked to become involved in a fraud that is occurring.¹

Crimes That Meet The "CALL FOR SERVICE" criteria

- 2.7 The Home Office Counting Rules state that the local Police will record all the following fraud offences as though reported to Police by the NFIB:
- Offences where offenders are arrested by Police, or
 - Where there is a call for service to Police and the offender "is committing" or has recently committed,
 - At the time of the call for service for all fraud types, or
 - Where there is a local suspect (see below).

'Local Suspect'

- 2.8 'Local suspect' is where through viable investigative leads;
- Police can, or could, locate a suspect with the details provided, or
 - Have there are sufficient details to apprehend an offender.
- 2.9 Local has its everyday meaning and has been used to ensure that as for any other type of crime, where there are local viable investigative leads police should consider the crime for investigation. *This is intended to provide the same policing response as with other crime types.* For example: If

¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/796319/count-fraud-apr-2019.pdf

following an assault, a suspect can be apprehended, police could respond to that policing demand. It is intended that it should be the same for fraud offences.

- 2.10 Where this is not the case and the crime needs to be transferred, the crime should be passed to the NFIB or referred to Action Fraud if appropriate. The NFIB will then deal with the report in the same way as with any other reported crime. The Home Office counting Rules do not guarantee an instant police response or investigation and when trying to obtain assistance under them you may find that you need to make a case through argument for intervention, but they are useful to be aware of when a fraud is actually occurring.

3.0 WHAT HAPPENS WHEN A REPORT IS RECEIVED BY ACTION FRAUD

- 3.1 Due to the volume of reports that Action Fraud receive, and the fact that not all reports will contain viable leads for investigation, it is not feasible for NFIB staff to look at every crime report. Instead two automated approaches are used to identify the cases that (in theory) are most likely to have viable lines for enquiry:

- A scoring matrix, which automatically scores crimes based on the presence or absence of certain information, such as suspect's bank account details, telephone number, or vehicle registration. Crimes with this information score higher than crimes without.
- Additional 'manual review' criteria, which the system uses to automatically identify any other cases that NFIB has determined should be reviewed. These are based on matters such as level of monetary loss (any losses over £100k should be reviewed), or the type of crime reported (e.g. pension liberation fraud). These crimes are reviewed because of the potential severity of impact on the victim, and to develop the intelligence picture and support collaborative activity.

- 3.2 All crimes are automatically assessed according to the scoring matrix, and the manual review criteria. The system then flags any crime that meets either the scoring matrix threshold, or one (or more) of the manual review criteria, to NFIB to be reviewed by a Crime Reviewer. Crime Reviewers then decide whether to send the case to a local police force for further investigation/enforcement.

- 3.3 Of the reports that are received by UK police through Action Fraud reported to the Home Affairs Select Committee, that during 2016/17 there had been over 260,000 reports² of fraud made of which 71,133 were disseminated to police forces for action. *The Times* reported in May that only cases involving losses of over £100,000 are being passed to a human investigator, with others being "dismissed by a computer algorithm as unworthy of investigation".³

- 3.4 Her Majesty's Inspectorate of Constabulary (HMIC) investigated territorial forces response to Action Fraud disseminated crime packages and looking at six out of the 43 forces, found "very few police officers and staff who understood either their own roles and responsibilities or those of their force in relation to the investigation of fraud." HMIC found a particularly poor level of knowledge, at all ranks, of the functions of Action Fraud and the NFIB. It also criticised an "absence of strategic leadership and direction" on digital crime in all but one of the forces examined.⁴

- 3.5 However not all of the 'packages' sent to UK territorial forces resulted in a court outcome. The figures given in the report show that of the 71,133 reports disseminated during 2018, 37,632 (53%) resulted in a Home Office outcome (caution etc.) whilst a further 29,418 (41%) resulted in a non-judicial outcome and only 8,214 (11%) were tested in court. Of the total number of over 260,000 reports received this represents just over 3% of all reports.

² <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51507.htm> see paragraph 57.

³ *The Times*, Cybercrime victims forced to use private investigators, 21 May 2018

⁴ HMIC, *Real lives, real crimes: A study of digital crime and policing*, December 2015

- 3.6 Meanwhile in September 2018 the consumer magazine 'Which' reported that 96% of cases reported to Action Fraud go unsolved.⁵ The magazine continued by saying that less than one in 20 crimes handled by Action Fraud results in a conviction. 'Which' concludes that *"comparing our research with other crime statistics shows that police solve significantly less fraud cases than any other crime group. Alarmingly this comes as fraud offences continue to rise. UK residents are now more likely to be victims of fraud and cybercrime than any type of offence, according to the ONS. Fraud and cybercrime offences are now ten times more common than burglary."*

4.0 INDUSTRY REQUIREMENTS

- 4.1 There isn't a specific requirement to report fraud under the CAA ATOL Regulations themselves. But the ATOL Standard Terms that apply to all ATOL holders include the following:

"The ATOL holder will immediately inform the CAA if the ATOL holder becomes aware it, the ATOL holder's group or a related party is the subject of an investigation whose findings, if these were unfavourable to the ATOL holder or the ATOL holder's group, would have a material impact on the financial resources of the ATOL holder or the ATOL holder's group."

- 4.2 This is really aimed at making an ATOL holder tell the CAA if they are on the wrong side of an audit/accounting report, but this could also be applied to a fraud investigation. And the CAA does encourage the trade to bring suspected illegal trading to their notice via enforcement@caa.co.uk. And there's also the CAA's whistleblowing web page: <http://www.caa.co.uk/default.aspx?catid=1&pageid=9487>.

ABTA & The Travel Network Group

- 4.3 ABTA and The Travel Network Group currently do not have an explicit requirement for their member companies and organisations to report fraud or any fraud investigation to them directly. However, it is advisable to keep them informed of any fraud that does occur as they can render valuable assistance.

Advice & Assistance

- 4.4 Prevention of Fraud in Travel can provide practical advice on a fraud that has occurred or is occurring and can seek direct help from the police or other partners if required. If you need assistance let us know through contactus@profit.uk.com.

Contact us

Prevention of Fraud in Travel (PROFIT) - contactus@profit.uk.com

Fraud Intelligence Network (FIN) - contactus@fraudintelnet.co.uk

The FIN Tool

- 4.5 Fraud data entered by companies using the FIN counter fraud intelligence tool is accessible to the police via the NFIB and useful to all system users.

Next Week: Part 8 Preparing For Court

⁵ <https://www.which.co.uk/news/2018/09/exclusive-more-than-96-of-reported-fraud-cases-go-unsolved/> - Which?