Internet Telephony Services Providers' Association

ITSPA Telephony Fraud – Reporting Guidance

May 2015

Contact: team@itspa.org.uk

Telephony Fraud – Reporting Guidance

CONTACT
For more information, please contact:

ITSPA Operations Working Group
team@itspa.org.uk
+44 (0)20 3397 3312

Telephony fraud is a large and increasing problem for the industry - estimated to cost $46bn per year globally. Our members tell us that fraud is one of the most significant problems they now face but unfortunately successful frauds routinely go unreported. This is for several reasons:

- A view that nothing will be done if it is reported
- Not knowing how or where to report it
- Fear of reputational damage from admitting fraudulent usage of their systems
- Uncertainties regarding whether Communications Providers can report on behalf of their clients or not.

As a result the full scale of the problem is not brought to the attention of the police and resources are not allocated to fight it. Consequently ITSPA has been working closely with ActionFraud to create a method of reporting fraud that is simple, fast, secure and anonymous.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

It is ITSPA's aim to increase the accurate reporting of fraud so that the true scale of telecoms fraud involving ITSPs and their customers is known, the Criminal Justice System takes the scale of fraud seriously and that resource will be aimed at those responsible for investigating these crimes and ultimately lead to a greater level of convictions for telecoms fraud related offences.

Types of Fraud

Whilst at least forty distinct types of telephone fraud are known to ITSPA, it is important that for reporting purposes, these are narrowed down to three distinct categories known to ActionFraud. These are:

- **Hacking PBX**: A remote attack on a telephone system. To gain from diverting calls to other destinations. It is also possible for someone with lawful access to the system to commit this offence by acting beyond their permissions.

- **Telecom Industry Fraud:** Where contracts are obtained by false representation from service providers either by using false details and/or providing bank account details, with no intention of paying the contract.

- **Cheque, Plastic Card & Online Bank Accounts (not PSP) – (for the purposes of this industry)** Where contracts are obtained by false representation from service providers either by using false details or stolen documents **and** supplying a cloned/compromised or stolen credit card with no intention of paying the contract

*****All Telecoms fraud should be reported to ActionFraud using one of these three categories*****

Registering for the ActionFraud Online Business Reporting Tool

ActionFraud offers telephone helpline for reporting fraud (0300 123 2040) however we strongly recommend that you register for the online tool which speeds up the reporting process significantly:

1. Visit www.actionfraud.police.uk
2. Click on "Report Fraud"
3. Click on "Business Reporting Tool"
4. Register with your email address, name and company name. For the free-field box, put "For reporting telephony fraud against us or on behalf of our clients"

ActionFraud will respond to the request and contact you with any appropriate questions before giving you access to the tool. This can take up to ten days.

Next Steps

Once you have access to the Business Reporting Tool, you will be able to file fraud reports quickly and efficiently.

Below we have included screenshots to clearly state how telephony fraud should be categorised and reported using the tool.

Login to

https://app03.actionfraud.police.uk/report/Account

using your login details provided by ActionFraud

About ITSPA

Founded in 2004, ITSPA is a membership-led organisation that represents predominantly network operators, service providers and other businesses involved with the supply of VoIP and unified communication services to business and residential consumers within the UK.

ITSPA helps act as the voice for the sector to key stakeholders; ensures that standards created by or imposed on industry are fair; leads on developments of best practice; campaigns on key issues that members face, promotes competition and self-regulation and serves as the leading networking forum for the UK VoIP industry with events throughout the year (including the annual industry awards – www.itspaawards.org.uk)

About ActionFraud

ActionFraud is the UK's national reporting centre for fraud and internet crime. You should report fraud to them if you have been scammed, defrauded or experienced cyber crime. ActionFraud provide a central point of contact for information about fraud and financially motivated internet crime. People are scammed, ripped off or conned everyday and we want this to stop.

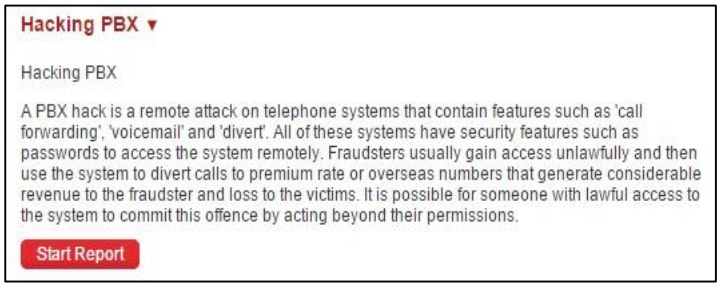
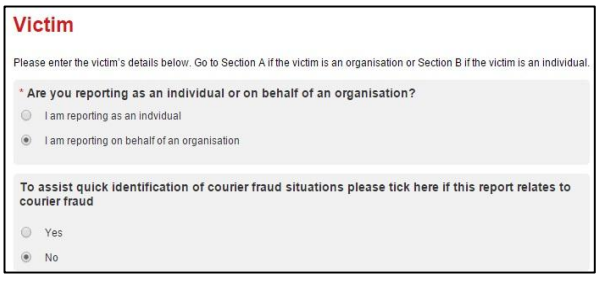
The service is run by the City of London Police along with the National Fraud Intelligence Bureau who are responsible for assessment of the reports. The City of London Police is the national policing lead for economic crime.

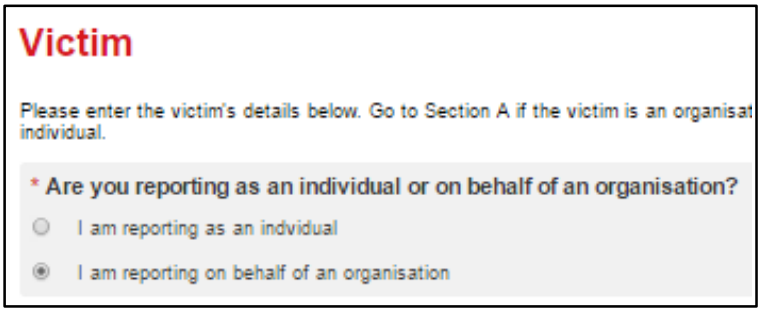
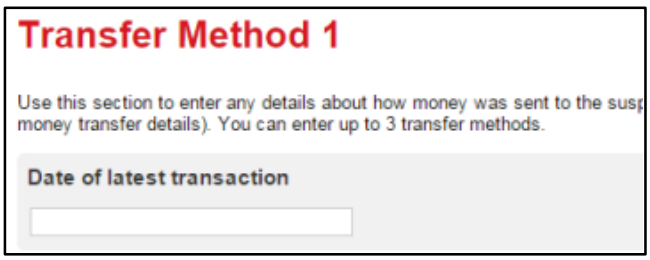
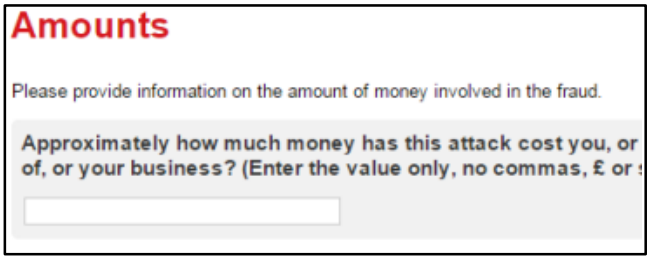
Once a report has been ingested from Action Fraud into the NFIB's database it goes through two automatic processes. Firstly the report will look to 'link' with any other reports that detail the same suspect entities. The report, or network of reports will then have a score applied to them.

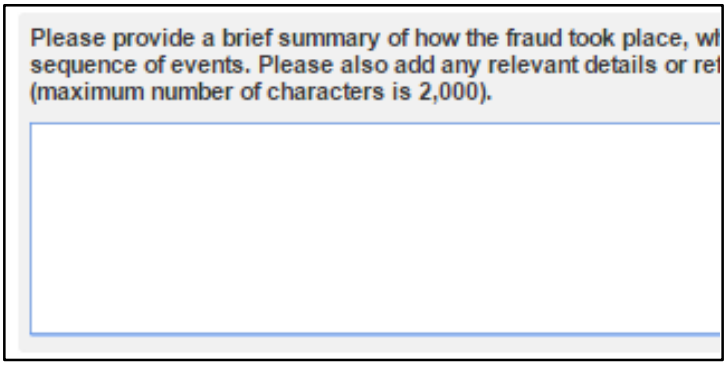
Scoring within the system is all based on how viable it is for UK Law Enforcement to carry out an investigation. If a report scores above the vailbility threshold it will then go into a queue to be reviewed by a Crime Reviewer. If the Crime Reviewer can corroborate the data in the report/s they will disseminate a package to the most appropriate Police Force or Law Enforcement Agency.

All reports of financially motivated cyber crime, e.g. 'PBX Hacking' are reviewed, regardless of whether the report has networked or scored.

Action Fraud Reporting Steps

Step	Notes	Screenshot
1	If a contract has been obtained, what payment method was provided by the suspect/s?	**Direct debit via a Bank account –** choose fraud category 'Telecom Industry Fraud' **Credit Card –** choose fraud category 'Cheque, Plastic Card & Online Bank Accounts (not PSP)'
2	If a PBX has been Hacked choose: (of the 56 categories, ITSP's use this one most of the time)	
3	If the crime affected you or if you have permission to report the crime affecting a third party choose "Crime." If you do not have permission to report the crime affecting a third party, or you have information you would like to supply, choose "Information." Tick as many boxes as you have information regarding. Do not tick the CFS box, as this applies to Police only.	
4	Your details as an individual reporting Note, you can save your responses here if you are completing more than one report and it will save them for the entire session.	
5	For any of the chosen three offences the victim will always be an organisation. Choose "No" for Courier fraud question.	

6	Complete Section A 'The victim is an organisation'. All the questions are about the victim not you, so if a client PBX has been hacked and they will be paying you, they are the victim. If your systems have been breached and you are paying, you are the victim. If a client PBX has been hacked, but, as a gesture of goodwill you are writing off the debt, you do not become the 'Victim'. The client remains the victim as they were the specific intended victim.	
7	Information on the suspect if known. Frauds should be reported even if information on the suspect is vague or non-existent. Complete Section A if the suspect is an individual (2 pages) or Section B if the suspect is an organization. It is vital that you put any details known about the suspect/s in these fields as this will help with the 'networking' process. Please enter the most prolific incoming and outgoing numbers dialed. You can enter up to nine numbers by adding the extra detail on the additional suspects field, in the telephone number fields.	 
8	**Transfer Method** – Only relevant if you (or your client) have paid the suspect, otherwise skip.	
9	**Amounts –** If this was an attack which led to an unauthorised call spend, enter "PBX hack led to unauthorised call spend" Enter the retail value of the fraud, report of any money that was recovered.	

10	Complete as many details as possible. If the fraud is a PBX hack and the suspect is unknown, choose "Other" and "Hacked PBX" In this free text box, your text could include details such as Revenue Share. If recording a PBX Hack please fill in all the 'additional' boxes with destinations and numbers called, type of PBX Hacked, whether the fraudsters hacked the systems via stolen credentials or not and IP addresses used to perform the hack as well as the evidence you have.	
11	Enter details about how the suspect made contact initially, e.g. through identity fraud or anonymously via hacking	
12	Use the large free text field in the middle of the page to provide a summary of what has happened. If you are reporting 'Cheque, Plastic Card and Online Bank Accounts' fraud please enter the following reference in the free text field: **xxITSPAxx** If you have entered incoming and outgoing numbers on the suspects page/s please provide detail on whether the numbers were incoming or outgoing in this free text field	
13	Impact – Choose the most appropriate option if known. Can be skipped if unclear For "How did you find out about Action Fraud," Choose "Other"	
14	Reporting is now completed; you will be issued with a Crime Reference Number and a password (if you have recorded a crime report) which you should keep. You can now report additional frauds if applicable