ITSPA

Internet Telephony Services Providers' Association

ITSPA Telephony Fraud – Reporting Guidance

October 2015

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Contact: team@itspa.org.uk

Telephony Fraud – Reporting Guidance

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:

CONTACT
For more information, please contact:

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

➢ 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.

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)	**Hacking PBX ▾** Hacking PBX A PBX hack is a remote attack on telephone systems that contain features such as 'call forwarding', 'voicemail' and 'divert'. All of these systems have security features such as passwords to access the system remotely. Fraudsters usually gain access unlawfully and then use the system to divert calls to premium rate or overseas numbers that generate considerable revenue to the fraudster and loss to the victims. It is possible for someone with lawful access to the system to commit this offence by acting beyond their permissions. **Start Report**
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.	**Step 2 - What information can you provide ?** Select as many categories below that you are able to provide information on. The more information you can provide the increased likelihood of a prosecution of the offender(s). Report Type: ○ Crime ○ Information ☑ Person Reporting ☑ Victim ☑ Suspect 1 ☑ Transfer Method 1 ☑ Amounts ☑ Fraud ☑ CFS (Applies to Police Only) ☑ Impact
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.	**Person Reporting** If you are reporting on behalf of the victim, please insert your details below. **Your title** Please select ▾
5	For any of the chosen three offences the victim will always be an organisation. Choose "No" for Courier fraud question.	**Victim** Please enter the victim's details below. Go to Section A if the victim is an organisation or Section B if the victim is an individual. * Are you reporting as an individual or on behalf of an organisation? ○ I am reporting as an individual ● I am reporting on behalf of an organisation To assist quick identification of courier fraud situations please tick here if this report relates to courier fraud ○ Yes ● No

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.	**Victim** Please enter the victim's details below. Go to Section A if the victim is an organisat individual. * Are you reporting as an individual or on behalf of an organisation? ○ I am reporting as an individual ◉ I am reporting on behalf of an organisation
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.	SECTION A - The suspect is an individual **Suspect Title** [Please select ▼] SECTION B - The suspect is an organisation **Suspect Organisation Name** [ ]
8	**Transfer Method** – Only relevant if you (or your client) have paid the suspect, otherwise skip.	**Transfer Method 1** Use this section to enter any details about how money was sent to the sus money transfer details). You can enter up to 3 transfer methods. **Date of latest transaction** [ ]
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.	**Amounts** Please provide information on the amount of money involved in the fraud. **Approximately how much money has this attack cost you, or of, or your business? (Enter the value only, no commas, £ or** [ ]

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.	How did the fraudster initially make contact with the victim? Other ▼ If selected other above, provide details Hacked PBX
11	Enter details about how the suspect made contact initially, e.g. through identity fraud or anonymously via hacking	Did Hacking feature as an enabler ? ◉ Yes ○ No
12	For tracking proposes please enter xxITSPxx in the large free text field in the middle of the page as well as a summary of what has happened. 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	Please provide a brief summary of how the fraud took place, wl sequence of events. Please also add any relevant details or re (maximum number of characters is 2,000).
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"	What impact has this fraud had on the victim? ○ Severe - have received medical treatment as a result of this crime and/or at risk of bankruptcy ○ Significant - impacting on health or financial well being ○ Minor - only a small impact on either health or financial well being ○ Concerned about the fraud but it has not impacted on health or financial well being
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	**Report Complete** Your report CRN : NFRC15010089 Your password : Fb67L You can report another fraud or return to the main site. **Report another fraud**