Code of Practice for Fraud Mitigation
Including customer and provider prevention and action

1. Introduction

Triangle Networks Ltd is a business only provider, offering a range of internet and telecommunications services. A core service provided by Triangle is the management of Openreach analogue and digital lines, and calls made from these lines.

The following Code of Practice information relates to telephony call fraud, often known as 'phone-freaking' or 'dial-through fraud'. It has been provided as a result of increased fraudulent activity.

In the event of any suspected fraud, contact the customers service department on 0844 811288 or 01275 871122. Request that all outgoing calls are suspended immediately. Contact your telephone system maintainer and if at all possible, disable your telephone system's access to the telephone network.

2. Customer Vigilance

Overview

Telephony fraud happens most at certain times of the year/month/week/day. This is largely due to being times when staff are unavailable, and therefore unlikely to notice activity.

These include, but are not limited to:

- Bank holidays
- Weekends
- Seasonal holidays
- Evenings/night-time

There are also signs of fraud during hours, which if spotted can be an early indication of a problem. This is often a result of fraudsters testing system vulnerabilities.

Indications of fraudulent call activity:

1. Police report unexpected 999 calls from your office

2. Significant number of voicemails being left without full messages

Customer information and updates

- We provide relevant warnings to customers on telephone bills, to assist with the early detection of fraudulent activity.
- This code of practice is displayed on our website
- All information within this code of practice is reviewed quarterly
- When a customer raises a query regarding fraud, they receive a copy of this code of practice, to help them understand how Triangle Networks manage fraud prevention, detection and cost limitation.

3. Prevention

There are some simple steps that businesses and their provider/hardware maintainers can take to reduce or potentially prevent dial-through fraud. Triangle Networks encourage customers to decide on the most appropriate actions to be taken following consideration of their business needs, implementing them without delay.

All customers are advised on billing memo, to request any changes and keep records of these requests.

We recognise that some of these measures are restrictive, as such we will not automatically implement these options, but we recommend the following:

Maintainer actions:

PBX maintainers will have received bulletins from manufacturers and distributers to advise engineers how to lock-down access. Please ensure that you have discussed the security of your telephone system with your maintainer. The following steps will help to reduce the risk of fraud:

1. Barring 09 and international call traffic – Other destinations if not used
2. Lock down all access according to manufacturer's documented standards

Please note that many systems are accessible from the internet, or internal network. If a hacker manages to access your telephone system configuration tools, measures put in place by your maintainer will have little to no affect. As such, each step is not to be used in isolation. Provider and customer steps are equally as important.

Provider actions

Changes can be made to your call routing service and BT Openreach line features, barring calls that you want blocked. Please note that these changes may affect your telephony service, as such it is your responsibility to ensure your chosen options are added and tested regularly.

1. Call barring of international and premium rate with call carrier
2. Call barring of international and premium rate with Openreach (may affect call diversion services)

Customer actions:

1. Ensure passwords are complex e.g not 1234
2. Ensure that passwords are changed on a regular basis
3. Ensure passwords are kept in a safe place
4. Organise a maintenance agreement with a reputable provider so that you get regular updates
5. Ensure your supplier and maintainer have emergency contact details for your 'key-holders'.
6. Test a barred number each month, test using Openreach pre-fix also (1280 xxxxxxxxxx)

4. Triangle Networks Service Monitoring and Management

There are some actions that a service provider/reseller can take to ensure that risk is limited. Whilst these actions are not guaranteed mitigation steps, all actions will reduce risk. We carry out the following actions to ensure that fraudulent call traffic is identified as soon as it can be.

1. Manually monitor call traffic on all bank holidays and seasonal holidays
2. Keep records of telephone numbers and features being used
3. Cease unused 'Indirect Access' registration if a customer is no longer billed by us.
4. Ensure all providers used offer daily call data and have on record that they can stop call traffic if they identify possible fraudulent traffic.
5. Auto import call data each day collecting promptly after data availability times
6. Set billing alerts to identify unusual call traffic – emailing support team and customer
    - Test alerts using lower settings each month
    - Adjust to multiple levels to include all customers i.e. alert at £50.00, £200.00
7. Bill fraudulent call traffic at cost
    - Call data totals detailed
    - Ensure that fraudulent call traffic is collated in a raw data format
    - Raw call data compared to total invoice value for destination
    - Customer invoice reissued with call data at cost
    - Raw call data provided to customer if requested

As a number of these steps rely on third-party technology and carrier data, these are not guaranteed mitigation measures.

5. Further Services / Options Available

Overview

Additional protection is available through a number of options. As a service provider, it is our obligation to make you, the customer, aware of these. These options are summarised on the monthly billing information. These options will often carry additional costs.

1. **Voice over IP -** SIP call traffic can be monitored in real-time and as such, SP's can limit risk, using SIP for certain destinations. We recommend barring international and premium rate traffic over Openreach lines, using 'SIP' for those calls. We recommend a SIP call limit of circa £100.00 per day, to ensure a maximum liability.

2. **Spare Analogue Line –** A single line without a call diversion feature, cannot be used for dial-through fraud. As such it needn't have a call barring feature. A single analogue line is also useful for general power/PBX/ISDN or SIP failure and of course for making outgoing international calls if all other lines are barred.

3. **Call logging -** Call logging systems output data from a telephone system in real-time. Limits and alerts can be set to notify a customer when traffic occurs. Please contact your system maintainer who will confirm whether this service is available.

4. **Insurance -** Some insurance companies can insure against digital theft/fraud. Please contact your chosen insurance broker/provider who will provide options to you.

5. **Alternative call handling -** Calls can be forwarded to out of hours call answering services using line features (calls don't reach the telephone system), limiting the risk of voicemail hacking. For more information please contact us for approved partners.

6. **Voice firewalling -** Devices are available connecting PBX systems to lines, monitoring traffic, routing it by destination.