Preventing Misuse of Sub-Allocated and Assigned Numbers CCUK Best Practice Guide – April 2024

Introduction

Scams, fraud and nuisance calls are all serious problems that are at the top of the political and regulatory agenda. There is no single solution to resolve the problem, however there are a number of tactics available to help minimise it. These tactics range from proactive measures (such as call blocking and caller verification) to reactive measures (including reporting incidents of fraud to the relevant authority and retrospectively blocking service).

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312
@commscounciluk

The following guidance is created for CCUK members to help you understand your obligations towards the proactive measure of understanding your customers and what they are using your numbers for. This is considered a critical step towards making it more difficult for scammers to get hold of phone numbers and telephony services.

The guidance is broad, in order to cover members of all sizes and all types of value chain. It is for you to decide which recommendations are suitable and proportionate for you to carry out with your own customer base. We strongly recommend that you document your own processes and procedures so that you can demonstrate your compliance.

Policy background

In November 2022, Ofcom issued a statement reminding providers of their existing obligations under General Condition B1, alongside guidance to help develop good practice to prevent the misuse of sub-allocated and assigned numbers. See Ofcom's full statement and the guidance.

Below we summarise the key points that all of our members should be aware of if they assign, sub-allocate or use numbers from the National Numbering Plan.

Why this guidance is necessary

All providers are required under the GCs to ensure that any numbers that they allocate or sub-allocate are used in accordance with the National Telephone Numbering Plan and other requirements concerning efficient use and management of numbers.

However, Ofcom recognises that further clarity and specific guidance could assist providers to meet their obligations, which in turn would reduce the occurrences of misuse of numbers, particularly scam and nuisance call activity. Ofcom is likely to check compliance with the best practice guidance when considering if a provider is complying with its regulatory obligations.

Key actions expected of all providers

1. Carry out robust due diligence checks before sub-allocating or assigning numbers;
2. Have a process to identify where the risks of misuse of numbers is higher;
3. Ensure your contracts enable you to meet your regulatory obligations;
4. Keep risk levels posed by business customers under review by monitoring for potential misuse; and
5. Define a process for responding to reports of potential misuse.

The guide below contains suggestions to help you comply with these expectations. This guide is specifically targeted at any provider who sub-allocates or assigns numbers "for the purposes of, or in connection with, a business" except for the points around responding to incidents of misuse, which apply to all types of end user.

Due diligence checks

You must take reasonable steps to understand your customer and the risk of misuse of numbers assigned to them. The checks required will depend on the nature of your relationship with your customer. For example, if they are a long-standing customer, you may not need to repeat your checks each time you assign numbers, but for a customer who is reselling numbers in a complex market, more extensive checks may be required. Below are the expectations of what checks and actions you should do.

1. 'Know your customer'

These include:

- Registering full company details, including trading names and registered office address;
- Fully understanding the nature of their business;
- Recording their existing telephone numbers and business websites;
- Finding contact details of the senior manager with responsibility for numbering; and
- Compiling information about the business customer's network and services provided

It is also likely to be appropriate to carry out more detailed checks by doing some or all of:

- Using the Companies House register to—
    - confirm that the information matches what you have been told;
    - check that the person acting as a director has not been disqualified;
    - check the details of all individuals with influence in the business;
    - check the details of individuals who receive a share of the revenue generated by the business; and
    - gather the names and details of any parent or holding company
- Asking the customer to confirm that no other party is operating as a shadow director;
- Checking the Cifas register to ensure that the person you are dealing with is not listed;
- Checking the Financial Conduct Authority (FCA) register to ensure that the customer has permission to carry out regulated financial activity;
- Checking with Phone-paid Services Authority (PSA) for banned individuals/companies;
- Checking if the business has links to any other current or previous accounts with you;
- Check the Individual Insolvency Register to see if influential individuals have gone bankrupt or agreed a deal to manage debt; and
- Check for relevant industry registrations.

2. Checks on the intended use and management of numbers

Actions that you should take include:

- Checking that the volume of numbers requested is consistent with the intended use of the numbers;
- Checking the customer's processes for sub-allocation and assignment to their customers;
- Obtaining the contact details of a senior manager who will act as a point of contact for discussing any issues relating to misuse; and
- Having a process for determining what scrutiny will be given to requests for additional numbers.

3. Identify high-risk customers

Ofcom has included examples of things that might flag a customer as high risk and so expect you to take extra precautions and carry out additional monitoring. Examples include:

- Adverse information from a public database (e.g. Cifas or FCA);
- Inaccurate, vague or unclear information provided about the numbers' intended use;
- The request for numbers not matching the intended use of numbers (e.g. requesting too many numbers for the intended use);
- Incorrect or incomplete information (such as address information);
- Not using a UK IP address when the business purports to be based in the UK;
- Signing up outside business hours (possibly in an attempt to circumvent checks);
- Name, address, postcode, IP address or other information which matches a disabled or dormant account already on your system;
- The use of generic, non-business email addresses or using the same email address for multiple accounts;
- Frequent changes in payment information;
- The service being provided by your customer appearing to have minimum checks in place for their own due diligence; and
- The use of a virtual private network (VPN).

4. Managing the due diligence process

As a provider, you must keep a record of the checks you carry out and have appropriate governance in place to ensure that the checks are carried out in accordance with your processes. Ofcom suggests that a senior manager be assigned responsibility for compliance.

If potential risk is identified, this senior manager should be responsible for both making a decision and for documenting the reason for that decision should it be challenged.

All individuals involved in the process of sub-allocating and assigning numbers should be trained in best practice and the procedures to be followed.

Continued Compliance

As well as initial onboarding checks, it is important that providers have processes in place to reassess the risk of number misuse after numbers are allocated or sub-allocated, including:

- Contractual controls – Set your contract out in clear terms to ensure compliance with all regulations and guidance. You should also consider requiring your customers to set out similar obligations in the contracts they provide to their customers.
- Reassessing risk as appropriate – This may include monitoring traffic patterns, compliance with CLI guidance, and being aware of complaints. You should consider repeating checks if there are changes to your business's structure or ownership.

Incidents Of Misuse

Providers must also have a process in place to deal with non-compliance situations. We suggest that members document their process and what will trigger it to be followed, again ensuring that all relevant employees are aware of the steps to be taken.

In the event of misuse, the priority becomes responding proactively and quickly to reduce potential consumer harm. Ofcom makes it clear that, although the best practice guide was mostly aimed at business users, the level of response required in a case of misuse applies to *all* users – including consumers. They also note in the guidance that it may be appropriate to withdraw or suspend service and numbers.

1. Providers' responsibilities to investigate incidents of suspected misuse

You should take the following steps to comply:

- Develop and maintain a process for handling complaints, being sure to maintain records of any investigations you carry out;
- Ensure that you can be contacted quickly and easily to be notified of suspected misuse;
- Ensure you take appropriate action to investigate and resolve incidents of suspected misuse in a timely manner and relative to the severity of the incident.

2. Providers' responsibilities in relation to evidence of misuse and responding to it

It is up to you to weigh up the evidence and take "necessary and proportionate action". Evidence includes complaints, appearing on warning lists and reports from law enforcement. Once you have identified misuse, you must take steps to prevent further potential misuse as far as reasonably possible. This might include invoking contract conditions on your customer and blocking calls. The action taken should be proportionate to the evidence and the risk posed.

Affected consumers should be supported as appropriate, and you must cooperate with Ofcom and other relevant organisations. If you are sub-allocating numbers, you should also consider informing the range holder of any incident.

If you have evidence of criminal activity, notify law enforcement. For immediate risk of harm or loss to a customer, call 999. In other cases, contact ActionFraud online, or call 0300 123 2040.

Range holders should also consider reporting to Ofcom if an incident has resulted in significant harm, if there are repeated incidents, or if the provider has not carried out an investigation in a timely manner. If you are unsure who to contact at Ofcom, please contact CCUK, and the Secretariat team can put you in touch with the correct contacts.