# Good practice guide to help prevent misuse of sub-allocated and assigned numbers

Annex 2

**GOOD PRACTICE GUIDE:**

Publication Date: 15 November 2022

# Contents

## Section



## Annex

# 1. Overview

Protecting consumers from harm is a priority for Ofcom. We continue to be concerned about the ongoing problem of scams facilitated by calls and texts.[1]

A common tactic is for scammers to contact people using a call, often claiming to be from legitimate organisations to trick their victim into providing personal details or making a payment. Using a valid telephone phone number adds to the legitimacy of the scam.

Ofcom is responsible for the administration of the UK's phone numbers under the Communications Act 2003. Phone numbers are allocated by Ofcom to telecoms providers, who can then transfer the numbers to other businesses or individuals. We have rules in place that set out the responsibilities on those transferring and using numbers.[2] However, we have identified inconsistencies and gaps in current practices, particularly in the checks providers carry out on customers requesting numbers and their response when alerted to the use of those numbers for scams.

This document comprises a good practice guide (the Guide) setting out the steps we expect providers to take to help prevent valid telephone numbers being misused, including to facilitate scams. This will provide more clarity for providers on how we expect them to meet their existing obligations under our rules. Where providers have these measures in place, it will be harder for people who intend to misuse numbers to access them, helping to reduce harm to consumers from scam calls. In our investigation of cases involving misuse of numbers, we would expect to take the Guide into account in considering whether enforcement action is appropriate.

[1] See Ofcom, March 2021. Ofcom's plan of work 2021/22, page 16.
[2] General Condition B1 of the General Conditions of Entitlement.

# 2. Background and introduction

2.1 Ofcom is responsible for the administration of the UK's phone numbers under the Communications Act 2003 (the Act). In carrying out our telephone numbering functions, we have a general duty to ensure that the best use is made of phone numbers and to encourage efficiency and innovation for that purpose.[3]

2.2 When allocating numbers to providers, Ofcom seeks information from the applicant which explains their proposed activities and how their network will operate. This will include, for example, how the applicant will interconnect with other networks and whether the services the applicant intends to offer are appropriate to the number ranges applied for and in accordance with the rules in the National Telephone Numbering Plan.[4] Additionally, we ensure contact details are provided for a named individual within the applicant's organisation. This information check is repeated every time numbers are applied for.

2.3 Once numbers are allocated, the provider is subject to Ofcom's General Conditions (GCs) including GC B1 which includes requirements to ensure numbers are used effectively and efficiently.

2.4 Providers allocated numbers by Ofcom ("range holders") are able to sub-allocate those numbers to other providers and resellers ("sub-allocatees") or assign them to end-users. Sub-allocated numbers may be further sub-allocated or assigned, and other providers may manage connectivity on the sub-allocatee's behalf.

## The purpose of this guide

2.5 This Guide sets out the steps we expect providers to take when sub-allocating and assigning numbers. Many of the measures are based on practices that some providers already have in place, and we see the Guide as consolidating and sharing best practice. It does not create new obligations but is intended to help providers ensure that they comply with their existing obligations under GC B1. In using this Guide, we would expect providers to take the steps that are reasonable and proportionate for their particular circumstances.

2.6 The Guide is part of our work to disrupt scams. When contacting consumers by phone, scammers often claim to be from legitimate organisations as part of their method of tricking their victim into providing personal details or making a payment. Having access to a valid phone number adds to the scammer's perceived legitimacy. If providers have processes in place to reduce access to valid numbers by those who intend to misuse them, and respond appropriately when misuse is reported, this should help reduce harm to consumers.

2.7 In our investigation of cases involving misuse of numbers, we would expect to take the Guide into account in considering whether enforcement action is appropriate.

[3] Section 63 (General duty as to telephone numbering functions) of the Act.
[4] Ofcom, The National Telephone Numbering Plan.

# Regulatory framework

## General conditions

2.8 GC B1 (allocation, adoption and use of telephone numbers) sets out the terms under which providers may apply for, be allocated and adopt telephone numbers to ensure their effective and efficient use.

2.9 In particular, GC B1.6 provides that:

> Where Telephone Numbers have been Allocated to the Communications Provider, that provider shall secure that such Telephone Numbers are Adopted or otherwise used effectively and efficiently.

2.10 GC B1.8 requires that:

> The Communications Provider shall take all reasonably practicable steps to secure that its Customers, in using Telephone Numbers, comply (where applicable) with the provisions of this Condition, the provisions of the National Telephone Numbering Plan and the Non-provider Numbering Condition.[5]

2.11 GC B1.9 sets out requirements in connection with the transfer of use of allocated numbers:

> The Communications Provider shall not transfer use of Telephone Numbers from the National Telephone Numbering Plan unless:
>
> (a) the Telephone Numbers have been Allocated to the Communications Provider; or the Communications Provider has been authorised (either directly or indirectly) to Adopt those Telephone Numbers by the person Allocated those Telephone Numbers;
>
> (b) the Telephone Numbers are used in accordance with the National Telephone Numbering Plan; and
>
> (c) the Telephone Numbers are Adopted or otherwise used effectively and efficiently.

2.12 In addition to these requirements, providers also have obligations under GC C6 which require them to provide Calling Line Identification facilities so that recipients can identify the person calling them.[6]

## Misuse of communications networks and services

2.13 Ofcom has powers under sections 128 to 130 of the Act to take enforcement action against those who persistently misuse electronic communications networks and services. Misuse of electronic communications networks and services involves using a network or service in ways which cause or are likely to cause someone else, especially consumers, to suffer

[5] See Ofcom's Non-provider Numbering Condition.
[6] Ofcom has published a final statement on changes to GC C6 and the CLI guidance. See Improving the accuracy of Calling Line Identification (CLI) data

harm. Misuse is persistent where it is repeated enough for it to be clear that it represents a pattern of behaviour or practice, or recklessness, about whether others suffer the relevant kinds of harm.[7]

2.14 Under GC B1.18, Ofcom may withdraw an allocation of telephone numbers from a communications provider where:

> …
>
> (d) the Communications Provider has used a significant proportion of those Telephone Numbers, or has used such Allocation to a significant extent, inconsistently with this Condition, or to engage in fraud or misuse; or
>
> (e) Ofcom has advised the Communications Provider in writing that a significant proportion of those Telephone Numbers has been used, or that such Allocation has been used to a significant extent, to cause harm or a nuisance, and the Communications Provider has failed to take adequate steps to prevent such harm or nuisance.

## Scope of the Guide

2.15 The Guide sets out steps that we expect providers to take to help ensure their compliance with GC B1.6, GC B1.8 and GC B1.9. In particular, it sets out guidance for providers on steps to address the risk of telephone numbers being misused. The misuse of numbers, for example to facilitate scams, is not an effective and efficient use of numbers.

2.16 The Guide covers three areas:

- Section 3: Due diligence checks before sub-allocating or assigning numbers.
- Section 4: Ensuring continued compliance and reassessing risk after transfer of numbers.
- Section 5: Responding to incidents of misuse.

2.17 The Guide is not intended to be an exhaustive list of the steps that may be appropriate in order for providers to comply with the GCs. It does not replace any existing obligations but aims to provide more clarity on compliance with the existing requirements.

2.18 In using this Guide, providers will need to ensure they comply with their obligations under relevant data protection legislation and the Investigatory Powers Act 2016.

### Who the Guide applies to

2.19 This Guide, like GC B1, applies to all communications providers (referred to as 'providers' in the Guide). The term "communications provider" is defined in the GCs as meaning "a person who (within the meaning of section 32(4) of the Act) provides an electronic

[7] See Ofcom, December 2016. Persistent Misuse Statement. The statement sets out examples of forms of misuse including silent and abandoned calls, misuse for dishonest gain – scams, misuse of a CLI facility and use of allocated numbers in a way that is inconsistent with the designations and/or restrictions in the Numbering Plan.

communications network or an electronic communications service". It is particularly relevant for providers who are allocated numbers by Ofcom or sub-allocated numbers by another provider.

2.20 The Guide applies when those numbers are sub-allocated or assigned to end-users for use for the purposes of, or in connection with, a business.[8] In this Guide we refer to the sub-allocatee or business end-user as a "business customer". Where relevant, Section 5 of the Guide also applies where the end-user is a consumer.[9]

[8] Other than as explained in footnote 9, the Guide does not apply when numbers are assigned to 'consumers' as defined in our General Conditions and as set out in the glossary (Annex A1).
[9] A provider may receive information that a business customer or consumer is misusing a number. The term 'consumer' is used as set out in the glossary, see Annex 1. The principles set out in Section 5 will be relevant when responding to any incident of potential misuse.

# 3. Due diligence checks before sub-allocating or assigning numbers

3.1 Before sub-allocating or assigning numbers to business customers, providers should take reasonable steps to understand the customers who have requested numbers, and the risk of number misuse.

3.2 In this section of the Guide we set out examples of checks that we consider appropriate for providers to carry out before sub-allocating or assigning numbers to business customers, in order to identify cases where there is a risk of number misuse. In line with good practice, these due diligence checks should be considered each time numbers are sub-allocated or assigned to a new or existing business customer.

3.3 The types of checks and level of scrutiny required will depend on the nature of the relationship. For example, a relatively lower level of scrutiny might be appropriate for an existing business customer about whom the provider already holds relevant information; where the provider and the business customer interact on a regular basis; and where the provider is familiar with the customer's use of and need for numbers.

3.4 Numbers will be sub-allocated and assigned to business customers who intend to use them in different ways and the type of number use may also affect the appropriate level of due diligence checks. For example, a business customer intending to resell numbers might require additional checks compared to a business customer being assigned a single number for use in their business. Overall, we expect providers to take reasonable steps to ensure that sub-allocated and assigned numbers are used effectively and efficiently, given the context of their relationship with the business customer.

## Due diligence checks to carry out

### 'Know your customer' checks

3.5 As part of assessing whether numbers are at risk of being misused, providers will need to know who they are sub-allocating or assigning numbers to. The following basic information should be collected as part of any 'know your customer' checks.

### ‘Know your customer’ checks

- Registered company details, trading names and registered office address
- Nature of the business
- Existing telephone numbers and business websites
- Contact details of the senior manager[10] with responsibility for numbering
- Information about the business customer’s network and the services provided

3.6 These checks mirror those that Ofcom carries out before allocating numbers to range holders. Note that Ofcom’s checks have been developed in light of our existing relationships with range holders and the telecoms industry, and our key concern around ensuring the operational integrity of the telephone network.

3.7 However, sub-allocation and assignment of numbers will encompass a much broader range of business types and business customers and providers might not be familiar with all these business/customer types. This means that in assessing the likelihood of number misuse, we would expect that providers will need to do further checks, beyond those outlined above, to understand the business customer making a request for numbers. The exact nature of these checks will depend on the customer and the request being made.

3.8 Examples of additional ‘know your customer’ checks that may be appropriate for that purpose are set out below.

### Additional 'know your customer' checks that may be appropriate

- Checking the Companies House register to confirm:
  - the information provided matches that on the Companies House register (and consider investigating further if that information has changed recently);
  - a person acting as a director of the business has not been disqualified;
  - the key details of all individuals with influence over the business, such as owners and directors;
  - the details of all individuals who receive any share of the revenue generated by the business customer; and
  - the names and details of any parent or ultimate holding company of the business customer.

[10] A senior manager is someone who is part of the organisation’s management team with appropriate powers to take decisions related to compliance, regulation and in particular numbering-related issues.

- Asking for undertakings from the business customer that no other party is operating in the capacity of a shadow director, as defined under the Companies Act 2006.
- Checking against the Cifas register that the person you are dealing with is not registered on the fraud risk databases.
- Checking against the Financial Conduct Authority's (FCA's) Financial Services Register that the business customer and individuals you are dealing with have permission to carry out regulated financial activities, if relevant.[11]
- Checking Phone-paid Services Authority (PSA) tribunal adjudications for banned individuals and banned companies.[12]
- Checking if the business customer has links to any other active accounts or previously blocked accounts with the provider.
- Obtaining and verifying details of the place of business, including ensuring the geographical location of the place of business matches the information provided by the business customer.
- Checking the Individual Insolvency Register to see if individuals with influence, such as owners and directors, have gone bankrupt or signed an agreement to deal with their debts.[13]
- Relevant industry registrations e.g. FCA firm reference number.

## Checks on intended use and management of numbers

3.9 We expect providers to carry out checks relating to how the business customer proposes to use numbers that are sub-allocated or assigned to them. Good practice checks on the intended use and management of numbers by business customers are set out below.

**Intended number use and management checks**

- Whether the volume of numbers requested is consistent with the intended use of numbers.
- The business customer's processes for sub-allocation and assignment.
- The contact details of a senior manager at the business customer, who will act as a contact point to discuss any issues related to misuse.

## Due diligence checks when additional numbers are requested

3.10 Checks should be considered whenever numbers are requested. Providers should have clear processes setting out the level of scrutiny that will be required when additional numbers are requested by an existing business customer. For example, if only a small additional number request is made, then further checks may not be proportionate.

[11] See FCA Financial Services Register.
[12] See PSA Tribunal adjudications.
[13] See Individual Insolvency Register (IIR).

However, if a significant number request is made, then further checks should be carried out.[14]

## Indicators of high-risk business customers

3.11 When conducting checks, a provider may identify information that could indicate a high-risk business customer. Examples of potential indicators are set out below.

### Indicators of a potentially high-risk business customer

- Adverse information from a public database, such as the Cifas register or the FCA's list of unauthorised firms and individuals.[15]
- Inaccurate, vague or otherwise unclear information provided about the intended use of numbers.
- The request for numbers not matching the intended use of numbers (e.g. requesting too many numbers for intended use).
- Incorrect or incomplete information (such as address information).
- Not using a UK IP address where the business purports to be based in the UK.
- Signing up outside of business hours (scammers may try to access telecoms resource outside of business hours to circumvent checks).
- Name, address, postcode, IP address, or other information matching a disabled or dormant account with the provider.
- The same email address being used to open multiple accounts.
- Use of a generic, non-business email address.
- Payment information being changed frequently.
- The service provided by the business customer appearing to have minimal processes or checks in place for further sub-allocation or assignment e.g. an automated number allocation system where no due diligence checks are carried out.
- Use of a virtual private network (VPN).

3.12 It is important to note that individually each indicator may not identify a potentially high-risk business customer, but a combination of these indicators might do so.

[14] What is considered "small" or "significant" will vary taking into account the existing numbering resource a business customer has, as well as the intended use of the numbers, amongst other factors.
[15] See FCA Unauthorised firms and individuals.

**Example**

A provider receives an application for 5,000 geographic numbers. The applicant is a consultancy firm and states that its business is based in the UK, consists of five people and the numbers will be used for its business purposes. The Companies House registration matches the information provided by the applicant. However, the volume of numbers requested seems disproportionate to the intended use of numbers and size of the firm. Therefore, it would be appropriate to carry out further checks with the applicant.

3.13 Where potentially high-risk business customers are identified, providers should undertake further checks e.g. assessing the due diligence processes the business customer has in place for further sub-allocating or assigning numbers. Additionally, where high-risk business customers request additional numbers, providers should undertake further due diligence before transferring numbers, such as:

- reviewing whether any complaints have been received about numbers already sub-allocated to the business customer; or
- checking for any unusual activity involving the customer's numbers e.g. high volumes of calls/texts, particularly where the calls are short or frequently dropped.

## Managing the due diligence process

3.14 Providers should document the checks they carry out before sub-allocating or assigning numbers. Providers should also have appropriate governance in place to ensure that these checks are carried out as intended and record their risk assessments. We suggest that a senior manager is nominated, with responsibility for ensuring that numbers are sub-allocated or assigned in accordance with the provider's processes.

3.15 Having carried out appropriate checks, if a potential risk is identified, the senior manager should be responsible for making the decision about whether or not to sub-allocate or assign numbers. This decision and the reasons for it should be documented.

3.16 Providers should consider training covering the best practice in this Guide for individuals involved in the process of sub-allocating and assigning numbers.

# 4. Ensuring continued compliance and reassessing risk after transfer of numbers

4.1 Providers should have processes in place to reassess the risk of number misuse after numbers have been sub-allocated or assigned, and to address non-compliant behaviour. This section of the Guide sets out the ongoing monitoring and compliance providers are expected to do once they have decided to transfer numbers. We set out how providers should have appropriate contractual controls, keep their risk assessments under review and have procedures in place to address non-compliance.

## Contractual controls to ensure continued compliance

4.2 To help ensure ongoing compliance when numbers have been transferred, providers should set out clear and unambiguous terms in their contracts with business customers requiring that numbers are used by the business customer in compliance with GC B1, the Numbering Plan and the Non-provider Numbering Condition.[16] Where appropriate, contracts should also include an obligation that sub-allocatees take all reasonably practicable steps to ensure compliance by their customers.

4.3 If a provider has concerns that a business customer is failing to comply with its obligations, it should raise those concerns with the business customer in the first instance.

## Reassessing risk

4.4 Providers should also keep the level of risk posed by a business customer under review and monitor for the potential misuse of numbers. These reviews should be tailored to each customer and the relevant risks that have been identified.

4.5 When monitoring for number misuse, providers should consider routinely testing and/or monitoring specific risks associated with a particular business customer. For example, where possible, range holders may want to check the volume and duration of outbound calls generated by numbers sub-allocated or assigned to the business customer that are routed through the provider's network. The frequency of testing should be based on the level of risk associated with each customer. For example, a business customer with no history of number misuse may require less frequent monitoring than one with a history of number misuse, or one with minimal due diligence checks for sub-allocation.

4.6 Providers should also ensure that they comply with other obligations under the GCs, such as the obligations under GC C6 and the associated CLI guidance. These obligations require providers to ensure that the number being used is either a CLI from a number range that has been allocated to the originating network, or to seek assurance from their customer that they are using a CLI that they have permission to use (either because they have been

[16] See Ofcom's Non-provider Numbering Condition.

directly assigned the number or have been given permission by a third party who has been assigned the number).[17]

4.7 Providers should review their risk assessments, referred to in paragraph 3.14, on an ongoing basis and update them in response to significant changes to the commercial relationship between the provider and business customer. These may include, but are not limited to:

- the provider receiving complaints about the business customer's use of sub-allocated or assigned numbers which may indicate a change in the level of risk posed;[18]
- changes to the business customer's approach to meeting its obligations, such as the customer refusing to engage with the provider, being obstructive or reluctant to provide information; and
- major changes to the business customer's company structure e.g. buying or merging with another company, the creation of a holding company structure, appointment of new directors.

## Addressing non-compliance

4.8 Providers should have robust procedures in place to address non-compliant behaviour by business customers. For example, a provider may become aware that its sub-allocatee has received reports of number misuse but not taken action to investigate the reports. A provider should engage with its business customer to understand the nature of the problem and consider how to resolve it. This may involve increased monitoring and oversight of number use or, where appropriate, the suspension or withdrawal by the provider of numbers assigned or sub-allocated to the customer.

[17] See paragraph 4.13 of Ofcom, February 2022. Guidance on the provision of Calling Line Identification facilities and other related services.

[18] A business customer's compliance history may change after numbers have been allocated. There may be reports of misuse during the period of the relationship which may change the level of risk posed.

# 5. Responding to incidents of misuse

5.1 Despite a provider's commitment to compliance, incidents of misuse of numbers may still occur. Providers should respond proactively to any such incidents. This will help to ensure that where issues do arise, action is taken quickly and the potential for consumer harm is reduced. Where relevant, the guidance in this section applies to incidents of misuse where the number is being used by consumers as well as business customers.[19]

## Providers' responsibilities to investigate incidents of suspected misuse

5.2 Providers should develop and maintain a process for handling complaints related to potential and actual misuse of numbers. This should include maintaining a record of any investigations, outcomes and action taken in relation to such misuse.

5.3 Providers should ensure that consumers, other providers, regulators, law enforcement agencies, and other organisations and businesses are able to notify them quickly and easily of suspected misuse of numbers.

5.4 Providers should ensure that they take appropriate action to investigate and resolve incidents of suspected misuse in a timely manner, taking into consideration the severity, urgency and complexity of the issue. They should work with other providers and organisations, including law enforcement, as appropriate.[20] Complainants should be made aware of the outcome as soon as possible. Where appropriate we would also encourage providers to set target service level agreements (SLAs) for reviewing misuse reports.

## Providers' responsibilities in relation to evidence of misuse

5.5 It is a provider's responsibility to weigh up the evidence of misuse and take necessary and proportionate action. Evidence of misuse might include, for example, customer complaints about a particular number, complaints reported to Ofcom or a direct report from an organisation affected by an impersonation scam. We set out some examples of the indicators of number misuse below.

[19] A provider may receive information that a business customer or consumer, as defined in our General Conditions, is misusing a number, The principles set out in Section 5 will be relevant when responding to any incident of potential misuse (see footnote **Error! Bookmark not defined.**).

[20] In the UK, we do not have a Common Numbering Database. Therefore, when a number is reported for misuse, the report is usually made to the range holder. Providers will then share information to help determine the current holder of the number.

### Examples of evidence of misuse

A report from law enforcement, regulators or government agencies will likely provide stronger evidence than a single report from a consumer. However, a significant volume of complaints from consumers may suggest that a number is being misused. Some organisations may be able to provide a report with documentary evidence, such as cloned literature with fake contact details diverting the consumer from the legitimate organisation to the scammer. This could include fake websites or printed information packs with valid numbers for consumers to call. These reports will usually be made to the provider by the organisation which is being cloned.

5.6 Providers should also review scams-related information to ensure they are aware of the latest tactics used by scammers, such as:

- The FCA warning list;[21] and
- Latest scam trends published by various organisations such as Action Fraud, Which? and Age UK.[22]

5.7 A provider may also take into account information gathered as part of its due diligence checks of the business customer, such as the business customer's network setup and its use of numbering and networks.

### Example

A provider has assigned numbers to an end-user who will use them to make outbound calls only and they will not be used for inbound calls. The provider agrees that the business customer will also set up inbound call routing to play a message to any consumer who calls back, letting them know the purpose of the missed call. The inbound routing is suddenly stopped and the provider starts to receive reports of suspected misuse.

The provider should take this information into account when considering the likelihood of potential misuse and assessing the report made.

5.8 We expect providers to review and evaluate any evidence they receive of misuse, before taking appropriate action. For example, it is not sufficient on its own for a provider to refer the person reporting the issue to law enforcement.

## Responding to evidence of misuse

5.9 Providers should, as far as reasonably possible, prevent any further potential misuse once they have been informed or have identified a potential concern.

5.10 To prevent further harm to consumers, providers may wish to use the contractual controls that have been built into their agreements to ensure that sub-allocated or assigned

[21] FCA warning list
[22] Action Fraud; Which?; Age UK

numbers are prevented from being misused. This may include requiring urgent action from a business customer in response to a complaint; applying temporary blocks to numbers or customer accounts; suspending some services (e.g. if the issue is related to outbound calls, outbound calls may be suspended but inbound calls continue as usual); or using contractual controls to withdraw numbers.

5.11 Any action taken should be proportionate to the evidence the provider has received and the potential risk posed to consumers.

**Example**

A provider receives a report that a number it is responsible for is being used in a live scam. This is a single report from a consumer. The provider decides to take no action as the consumer provides few details.

A few hours later it is contacted by a financial business which sends evidence to the provider that the number is being used to impersonate a financial service provider. The financial business provides details of the scam, and the literature being used by the scammers including the telephone number.

Based on the strength of the evidence received, the provider applies a temporary suspension to the account, blocking it from making or receiving calls. It contacts the account owner for further information, providing a 48-hour deadline to respond. The provider does not receive a response to the original or further contact and suspends the account.

5.12 Providers should also provide support and information to any affected consumers, and cooperate as appropriate with Ofcom, other regulators, law enforcement and other relevant organisations.

5.13 Providers are encouraged to proactively inform the range holder of suspected incidents of misuse of numbers. This should include providing details of the customer who misused the numbers, details of the incident and steps that have been taken to remedy the issue. If providers identify evidence of fraudulent or other criminal activity, the provider should notify law enforcement.

## The role of range holders

5.14 As part of any investigation into number misuse, we may contact the range holder even when the numbers have been sub-allocated to others, because Ofcom's direct relationships are with range holders. We would expect range holders to know who the numbers were sub-allocated to and have an understanding of the use of the numbers and the associated risks.

5.15 Once they become aware of any incidents of number misuse, range holders should also consider whether those incidents should be reported to Ofcom for potential enforcement action. Examples of incidents that it would be appropriate to report include:

- incidents that have resulted in significant consumer harm;
- repeat incidents involving a particular customer; and
- incidents where reports of misuse have not been investigated in a timely manner or otherwise dealt with appropriately.

## Reviewing and evaluating the processes

5.16 The tactics employed by scam callers are constantly changing. We encourage providers to keep up to date with industry developments and actively review their processes to ensure they remain robust. This should include updating their processes to incorporate lessons learned from previous incidents of misuse.

# A1. Glossary and abbreviations

**Assigned (in relation to phone numbers):** where numbers are transferred to end users i.e. individuals and businesses.

**Calling Line Identification (CLI):** means data that enables identification of the number from which a call could be made or to which a return call could be made.

**CLI authentication:** implementation of standards that make it possible for the network originating a call to confirm the caller's authenticity before passing it to the network of the person receiving the call.

**Consumer:** is defined in the General Conditions as meaning any natural person who uses or requests a Public Electronic Communications Service or Bundle for purposes which are outside his or her trade, business, craft or profession.

**Customer:** is defined in the General Conditions and, in relation to a Communications Provider, means the following (including any of them whose use or potential use of the network or service is for the purposes of, or in connection with, a business): (a) the persons to whom the network, service or Bundle is provided in the course of any business carried on as such by the Communications Provider; (b) the persons to whom the Communications Provider is seeking to secure that the network, service or Bundle is so provided; (c) the persons who wish to be so provided with the network, service or Bundle, or who are likely to seek to become persons to whom the network, service or Bundle is so provided.

**Do Not Originate (DNO) list:** a list, set up by Ofcom and UK Finance, of certain telephone numbers used only for inbound calls that would not be used to call consumers.

**End user:** is defined in the General Conditions and means in relation to a Public Electronic Communications Service or Bundle: (a) a person who, otherwise than as a Communications Provider, is a Customer of the provider of that service or Bundle; (b) a person who makes use of the service or Bundle otherwise than as a Communications Provider; or (c) a person who may be authorised, by a person falling within paragraph (a), so to make use of the service or Bundle.

**General Conditions (GCs):** conditions set by Ofcom under section 45 of the Communications Act 2003.

**Geographic number:** a telephone number that is identified with a particular geographic area.

**Impersonation scams**: where scammers claim to be from legitimate organisations to try to trick people into giving away personal details or making a payment.

**Non-geographic number:** any telephone number other than a geographic number

**Nuisance calls:** may include unwanted attempts to promote a product or service, as well as silent and abandoned calls. Nuisance calls are likely to cause annoyance, inconvenience and anxiety to consumers.

**Provider:** communications provider, defined in the General Conditions to mean a person who (within the meaning of section 32(4) of the Act) provides an electronic communications network or an electronic communications service.

**Range holder:** the provider to whom a particular number range or block has been allocated by Ofcom.

**Scam calls and texts:** calls and texts primarily aimed at defrauding consumers, either by tricking them into revealing personal details or into making a payment.

**Spoofing:** where callers hide their identity by causing a false or invalid phone number to be displayed when making calls. Those making such calls will create a phone number that appears like a phone number or may even mimic the number of a real company or person who has nothing to do with the actual caller.

**Sub-allocate:** where numbers are transferred by a provider to other providers or resellers.

**Unwanted calls:** calls that consumers do not want to receive. These can range from nuisance calls, through to scams.