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

A proposed guide for telecoms providers

[Good practice guide to help prevent misuse of sub-allocated and assigned numbers](#) – Welsh overview

CONSULTATION:

Publication date: 23 February 2022

Closing Date for Responses: 20 April 2022

Contents

Section

1. Overview	1
2. Background and introduction	3
3. Due diligence checks before sub-allocating or assigning numbers	9
4. Ensuring continued compliance and reassessing risk after transfer of numbers	14
5. Responding to incidents of misuse	16

Annex

A1. Responding to this consultation	20
A2. Ofcom's consultation principles	23
A3. Consultation coversheet	24
A4. Consultation questions	25
A5. Glossary and abbreviations	26

1. Overview

Protecting consumers from harm is a priority for Ofcom and we are concerned about the growing problem of scams facilitated by calls and texts.¹ The use of scam calls and texts is now widespread, with our research finding that suspected scam attempts affect the vast majority of people in the UK. Further, over the three-month period covered by our survey, we estimated that almost a million people followed the scammers' instructions in a message or call, risking financial loss and emotional distress if the scam attempt was successful. Even when not caught out by a scammer, people receiving attempted scams may experience annoyance and distress. Scams also impose costs on the wider economy, including the resources spent by legitimate businesses to support those customers that fall victim to fraud.

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 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 (the Act). 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.

In this document, we are consulting on a proposed good practice 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.

What we are proposing

The proposed guide sets out steps we expect providers to take to help prevent valid numbers being misused. We expect providers to have processes in place to ensure they know their business customers and how numbers will be used by them before numbers are transferred. We also expect providers to have processes in place to check customers are using numbers in compliance with the General Conditions, and for responding to reports of misuse.

¹ See Ofcom, March 2021. [Ofcom's plan of work 2021/22](#), page 16

² General Condition B1 of the [General Conditions of Entitlement](#).

In particular, we expect providers to:

- carry out a robust set of due diligence checks before sub-allocating or assigning numbers;
- have an approach for identifying where the risks of number misuse are higher;
- put in place contractual controls that enable the provider to meet their regulatory obligations;
- keep the level of risk posed by a business customer under review by monitoring for the potential misuse of numbers; and
- have an appropriate process for responding to reports of potential misuse.

Next steps

- 1.1 We invite responses to this consultation by 20 April 2022. Subject to considering the views and evidence submitted in responses, we aim to publish a decision on our proposals in Autumn 2022.
- 1.2 This proposed guide forms part of Ofcom's wider work to tackle scam calls and texts. Alongside our proposed good practice guide, we are consulting on proposals to strengthen our rules and guidance for providers to detect and block spoofed numbers.³ We have also added information to our website to explain the purpose of our 'Do Not Originate' (DNO) list and how to get in touch if you think you have numbers that should be added to the list.⁴ We will be considering whether the DNO list can be expanded to include numbers from a wider group of organisations.
- 1.3 We will carry out follow-up research into the incidence of call and text scams to help us monitor the impact of work that we and others are doing, including where to focus our efforts as scammers evolve their tactics. The research will also inform our continued work to raise awareness of scams and the steps people can take to protect themselves. We will also continue to collaborate with other organisations working to reduce scams as part of a coordinated approach.

³ Ofcom, February 2022. [Improving the accuracy of Calling Line Identification \(CLI\) data](#)

⁴ The information on our website can be found here: ['Do Not Originate' \(DNO\) list](#).

2. Background and introduction

Ofcom administers the allocation of numbers and regulates their effective and efficient use

How we allocate numbers

- 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.⁵
- 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. 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.

Problems that have been identified

- 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.
- 2.5 Through stakeholder engagement, we have found that there is considerable variation in:
 - how providers manage numbers, including their due diligence checks before sub-allocating or assigning numbers;
 - processes for ensuring their customers use numbers in compliance with the GCs; and
 - how they respond to reports of misuse.
- 2.6 Without appropriate processes in place for managing numbers, there is greater risk that numbers may be misused, for example to facilitate scams.

⁵ [Section 63](#) (General duty as to telephone numbering functions) of the Act.

The purpose of this guide

2.7 This proposed guide sets out the steps we expect providers to take when sub-allocating and assigning numbers. Many of the measures we set out 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.

Our good practice guide is part of Ofcom's work to tackle scam calls and texts

2.8 We are committed to working with partners to reduce the harm from scam calls and texts. The key elements of our response are set out below.

- We aim to **disrupt scams** by making it harder for scammers to use communications services to reach consumers. We propose to strengthen our rules and guidance, while at the same time supporting providers to develop their own technical solutions to detect and prevent scam traffic.
- Scams are increasingly complex, often involving different companies and sectors. So, a coordinated approach is vital to ensure more scam attempts are blocked or disrupted. We will **collaborate and share information** more widely, including with Government, regulators, law enforcement and consumer groups.
- Given the pace at which scammers change their tactics, we understand that it will not be possible to stop all scams reaching consumers. We are working to **help consumers avoid scams** by raising awareness so consumers can more easily spot and report them.

2.9 Our good practice 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 will help reduce harm to consumers.

Regulatory framework

General duties

2.10 Under section 3 of the Act, it is Ofcom's principal duty, in carrying out its functions, to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition.

- 2.11 In performing our duties, we are required to have regard to a number of matters, as they appear to us to be relevant in the circumstances, including the desirability of ensuring the security and availability of public electronic communications networks and services; the needs of persons with disabilities, of the elderly and of those on low incomes; the desirability of preventing crime and disorder; and the opinions of consumers in relevant markets and of members of the public generally.
- 2.12 We are also required to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed, as well as to the interests of consumers in respect of choice, price, quality of service and value for money.
- 2.13 Ofcom has a number of functions in relation to telephone numbers, which are set out in sections 56 to 63 of the Act. It has a general duty in section 63 of the Act to carry out its numbering functions in a way that ensures the best use is made of numbers, encouraging efficiency and innovation for that purpose. It also has a duty to publish the National Telephone Numbering Plan (the Numbering Plan) and to keep it under review. The Numbering Plan sets out telephone numbers that are available for allocation and any restrictions on how they may be adopted or used.⁶

General conditions

- 2.14 Ofcom's power to set GCs is set out in section 45(2)(a) of the Act. A general condition may be applied generally to every provider or to a provider of a particular description specified in the condition. In addition to the matters to which GCs may relate, which are set out in section 51 of the Act, Ofcom has specific powers to make GCs in relation to the allocation and adoption of telephone numbers in section 58 of the Act.
- 2.15 The matters to which GCs may relate include the imposition of restrictions on the adoption of telephone numbers by providers and requirements in connection with the adoption of telephone numbers. Section 56A(1) sets out that when Ofcom allocates telephone numbers in accordance with the Numbering Plan, it must specify whether an allocation may be transferred from one person to another and may set out the conditions under which the allocation may be transferred.
- 2.16 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.
- 2.17 In particular, GC B1.6 provides that:

⁶ Ofcom, December 2021. [The National Telephone Numbering Plan](#).

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.

2.18 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.⁷

2.19 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.

2.20 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.⁸

Misuse of communications networks and services

2.21 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 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.⁹

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

⁷ See [Ofcom's Non-provider Numbering Condition](#).

⁸ Ofcom is currently consulting on proposed changes to GC C6 and the CLI guidance. See Ofcom, February 2022, [Improving the accuracy of Calling Line Identification \(CLI\) data](#)

⁹ 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.

...

(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 proposed guide

- 2.23 Our proposed 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 proposes 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.
- 2.24 The following sections set out our proposed guide, which 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.
- 2.25 The proposed 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.
- 2.26 In using this proposed guide, providers will need to ensure they comply with their obligations under relevant data protection legislation and the Investigatory Powers Act 2016.

Who the proposed guide applies to

- 2.27 This guide, like GC B1, applies to all communications providers (referred to as ‘providers’ in the guide). The term “communications provider” is defined in section 405(1) of the Act as meaning “a person who (within the meaning of section 32(4)) provides an electronic 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.
- 2.28 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.¹⁰ In this guide we refer to the sub-

¹⁰ Other than as explained in footnote 11, 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 A5).

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.¹¹

Impact Assessment

- 2.29 Section 7 of the Act sets out Ofcom’s duty to carry out impact assessments. We have not carried out an impact assessment in respect of this consultation document. This is because an impact assessment was carried out when we introduced the relevant GCs, and we are now publishing a good practice guide to help providers comply with those existing obligations. Therefore, we do not consider that the contents of this consultation document impose any additional burdens on providers beyond those required under the GCs which they should already be meeting.

Equality impact assessment

- 2.30 Section 149 of the Equality Act 2010 (the 2010 Act) imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation. The 2010 Act also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not.
- 2.31 Section 75 of the Northern Ireland Act 1998 (the 1998 Act) also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom’s Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.¹²
- 2.32 To help us comply with our duties under the 2010 Act and the 1998 Act, we assess the impact of our proposals on persons sharing protected characteristics and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. We do not consider that our proposals have equality implications under the 2010 Act or the 1998 Act.

¹¹ 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 5. The principles set out in Section 5 will be relevant when responding to any incident of potential misuse.

¹² Ofcom, January 2014 (updated December 2019). [Revised Northern Ireland Equality Scheme for Ofcom](#).

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 proposed 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 manager¹³ 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.

¹³ 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.¹⁴
- Checking Phone-paid Services Authority (PSA) tribunal adjudications for banned individuals and banned companies.¹⁵
- 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.¹⁶
- 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.

¹⁴ See [FCA Financial Services Register](#)

¹⁵ See [PSA Tribunal adjudications](#)

¹⁶ See [Individual Insolvency Register \(IIR\)](#)

However, if a significant number request is made, then further checks should be carried out.¹⁷

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.¹⁸
- 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.
- 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.

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.

¹⁷ 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.

¹⁸ 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 that covers the best practice set out in this guide for individuals involved in the process of sub-allocating and assigning numbers.

Consultation questions

1. Do you have any comments on the suggested measures set out in Section 3?
2. Have you used any other due diligence checks that you think would be beneficial if adopted across the industry?

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.¹⁹ 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

¹⁹ See [Ofcom's Non-provider Numbering Condition](#)

directly allocated the number or have been given permission by a third party who has been allocated the number).²⁰

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;²¹
- 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.

Consultation questions

3. Do you have any comments on the suggested measures set out in Section 4?
4. Have you used any other ongoing checks to ensure compliance that you think would be beneficial if adopted across the industry?

²⁰ See paragraph 4.13 of Ofcom, May 2019. [Guidance on the provision of Calling Line Identification facilities and other related services](#). Ofcom is currently consulting on changes to GC C6 and the CLI guidance alongside this consultation. See Ofcom, February 2022. [Improving the accuracy of Calling Line Identification \(CLI\) data](#)

²¹ 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.²²

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.²³ Complainants should be made aware of the outcome as soon as possible.

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.

²² 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 11).

²³ 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;²⁴ and
 - Latest scam trends published by various organisations such as Action Fraud, Which? and Age UK.²⁵
- 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.

²⁴ [FCA warning list](#)

²⁵ [Action Fraud](#); [Which?](#); [Age UK](#)

- 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 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.

Consultation questions

5. Do you have any comments on the suggested measures set out in Section 5?

A1. Responding to this consultation

How to respond

- A1.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 20 April 2022.
- A1.2 You can download a response form from <https://www.ofcom.org.uk/consultations-and-statements/category-2/consultation-good-practice-guide-on-sub-allocated-assigned-numbers>. You can return this by email or post to the address provided in the response form.
- A1.3 If your response is a large file, or has supporting charts, tables or other data, please email it to scamsconsultations@ofcom.org.uk as an attachment in Microsoft Word format, together with the [cover sheet](#).
- A1.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:
- Scams Consultations
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA
- A1.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:
- Send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files. Or
 - Upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.
- A1.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential).
- A1.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt if your response is submitted via the online web form, but not otherwise.
- A1.8 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.
- A1.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex 4. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A1.10 If you want to discuss the issues and questions raised in this consultation, please send an email to scamsconsultations@ofcom.org.uk.

Confidentiality

A1.11 Consultations are more effective if we publish the responses before the consultation period closes. In particular, this can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish all responses on [the Ofcom website](#) as soon as we receive them.

A1.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A1.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A1.14 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our [Terms of Use](#).

Next steps

A1.15 Following this consultation period, Ofcom plans to publish a statement in Autumn 2022.

A1.16 If you wish, you can [register to receive mail updates](#) alerting you to new Ofcom publications.

Ofcom's consultation processes

- A1.17 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex A2.
- A1.18 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.
- A1.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A2. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

- A2.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

- A2.2 We will be clear about whom we are consulting, why, on what questions and for how long.
- A2.3 We will make the consultation document as short and simple as possible, with a summary of no more than two pages. We will try to make it as easy as possible for people to give us a written response. If the consultation is complicated, we may provide a short Plain English / Cymraeg Clir guide, to help smaller organisations or individuals who would not otherwise be able to spare the time to share their views.
- A2.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.
- A2.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.
- A2.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

- A2.7 We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish all the responses on our website as soon as we receive them. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A3. Consultation coversheet

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing

Name/contact details/job title

Whole response

Organisation

Part of the response

If there is no separate annex, which parts? _____

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name

Signed (if hard copy)

A4. Consultation questions

A4.1 The full list of consultation questions is set out here.

1. Do you have any comments on the suggested measures set out in Section 3?
2. Have you used any other due diligence checks that you think would be beneficial if adopted across the industry?
3. Do you have any comments on the suggested measures set out in Section 4?
4. Have you used any other ongoing checks to ensure compliance that you think would be beneficial if adopted across the industry?
5. Do you have any comments on the suggested measures set out in Section 5?

A5. 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.

CLI data: means the contents of all signalling messages which can be used between Communications Providers and/or between Communications Providers and End-Users to signal the origin of the call and/or the identity of the calling party, including any associated privacy markings.

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 section 405(1) of the Communications Act 2003 as meaning a person who (within the meaning of section 32(4)) 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.