Guidance for number range holders to prevent misuse of Global Titles

Annex 6

Published 22 April 2025

Contents

Section

1. Overview

1.1 Mobile operators use Global Titles (GTs) as routing addresses for the exchange of SS7 signalling messages between 2G and 3G mobile networks and to support their provision of mobile services.

1.2 GTs are created from the ranges of mobile numbers that we allocate to mobile operators. Mobile numbers that are used as GTs are used solely for this purpose and are not assigned to end users.

1.3 GTs normally underpin the provision of legitimate mobile services, but GTs can also be misused. We have identified evidence that some +44 GTs are a source of malicious signalling traffic affecting mobile networks and their subscribers which raises network security, privacy, reputation and fraud risks.

1.4 Malicious signalling can occur when mobile operators use GTs created from numbers allocated to them by Ofcom as inputs to services they provide to their customers.

1.5 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.

1.6 The misuse of GTs does not align with this duty or the obligations we have imposed on number range holders.[1]

1.7 This document constitutes Guidance for number range holders on their responsibilities to prevent misuse of their GTs. It sets out the steps we expect number range holders to take to prevent their GTs being misused. This will provide more clarity on how we expect number range holders to meet their existing obligations under our rules. When deciding whether to open an investigation into a number range holder relating to misuse of their GTs, and if so the type of action that may be appropriate, we expect to take this Guidance into account.

Introduction and background

1.8 In July 2024, we consulted on proposals designed to tackle malicious signalling originating from UK GTs.[2] Evidence gathered as part of that consultation showed +44 GTs[3] have been one of the most significant and persistent sources of malicious signalling traffic affecting mobile networks globally. The malicious signalling was partly originated from GTs that have been leased by number range holders, hence we proposed to ban the leasing of GTs to third parties.

[1] Number range holder / range holder refers to an operator with an allocation of numbers from Ofcom. See also paragraphs 1.29 and 1.30 below.
[2] Ofcom, 2024. Global Titles and Mobile Network Security - Ofcom.
[3] +44 numbers have been allocated to both UK operators and to operators in the Crown Dependencies, i.e. the Bailiwicks of Jersey and Guernsey and the Isle of Man. References to +44 GTs are references to GTs used by both Crown Dependency and UK operators and references to UK GTs are references to GTs used by UK operators only.

1.9 Evidence also showed malicious signalling has arisen from GTs that were not leased meaning it may have arisen in connection with a service provided by a number range holder to its customer that uses a GT as an input.[4]

1.10 In April 2025, we published our statement on Global Titles and Mobile Network Security. This statement tackled malicious signalling originating from UK GTs by amending our General Conditions of Entitlement (GCs), Non-Provider Conditions and the National Telephone Numbering Plan (NTNP). Specifically, our statement implemented the following decisions:

a) to ban the leasing of GTs to third parties by operators that hold UK numbers;
b) to ban third parties from creating or using GTs from sub-allocated numbers;
c) to strengthen our rules to prohibit the misuse of GTs by number range holders by:

- implementing a new Non-Provider Condition 2.4 to ensure the rules in our General Conditions relating to misuse of GTs by communications providers apply to all operators who might have access to GTs through their number allocations (regardless of whether or not they may be considered a "Communications Provider" within the scope of General Condition B1); and
- publishing new Guidance for number range holders on their responsibilities to prevent misuse of their GTs. This includes the steps range holders are expected to take to comply with GC B1.6 and B1.8 (or Non-Provider Condition 2.4) when they are providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling;

d) to strengthen our rules to prohibit the creation and use of Global Titles from numbers not allocated for use.

1.11 This document is the above-mentioned Guidance for number range holders on their responsibilities to prevent misuse of their GTs. It reflects the decisions we made in our April 2025 Statement.[5]

Regulatory framework

1.12 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.

1.13 We consider that a number range holder's failure to take reasonably practicable steps to prevent misuse when providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling, could be in breach of B1.6 and B1.8. To this end, we are making clear that we would in appropriate circumstances take enforcement action for breaches of B1.6 or B1.8 in the context of this form of misuse of GTs.

1.14 In particular, GC B1.6 provides that:

[4] Ofcom, 2025. – Statement: Global titles and mobile network security, see paragraphs 3.13-3.15.
[5] Ofcom, 2025. – Statement: Global titles and mobile network security.

> 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.

1.15 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 [GC B1, including B1.6], the provisions of the National Telephone Numbering Plan and the Non-provider Numbering Condition.

1.16 GC B1.18(d) and (e) give us the power to withdraw numbers where:

> The Communications Provider has used a significant proportion of those Telephone Numbers, or has used such Allocation to a significant extent, inconsistently with [GC B1, including B1.6 or B1.8], or to engage in fraud or misuse; or
>
> 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.

1.17 Condition 2 of the Non-Provider Conditions applies to all operators who might have access to GTs through their number allocations that may not be considered a "Communications Provider" within the scope of GC B1. Non-Provider Condition 2.4 requires that:

> Where Telephone Numbers are being used by any person, that person shall: (a) secure that such Telephone Numbers are used effectively and efficiently; and (b) take all reasonably practicable steps to secure that its Customers ensure the effective and efficient use of such Telephone Numbers.

1.18 In the event of non-compliance with Non-Provider Condition 2.4, we have powers under section 59(6) of the Act to take enforcement action against operators via civil proceedings. We also have the power to withdraw numbers under section 61(4) of the Act.

1.19 In accordance with sections 128 to 130 of the Act, we also have powers to take enforcement action against providers or other persons who persistently misuse an electronic communications network or service, including issuing a penalty of up to £2m. Misuse of an electronic communications network or service involves using a network or service in ways which cause or are likely to cause someone else, including consumers, to unnecessarily suffer annoyance, inconvenience or anxiety. 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. Any enforcement action for Persistent Misuse would take into account Ofcom's Persistent Misuse statement.[6]

[6] See Ofcom's Statement of policy on the persistent misuse of an electronic communications network or electronic communications service.

1.20 Section 5 of our April 2025 Statement explained in more detail the range of powers we have to take enforcement action in the context of this form of misuse of GTs.

The purpose of this Guidance

1.21 This document provides guidance to number range holders to prevent misuse of their GTs and ensure that their signalling capabilities are used for legitimate purposes.

1.22 It sets out the steps that we expect number range holders to take when providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling.

1.23 Number range holders should already have processes in place to comply with their numbering obligations, and we see this Guidance as consolidating and sharing best practice. It does not create new obligations but is intended to help number range holders ensure that they comply with their existing obligations under GCs B1.6 and B1.8 and Non-Provider Condition 2.4. This Guidance refers to GCs B1.6 and B1.8 and Non-Provider Condition 2.4 as relevant numbering rules.

1.24 If number range holders have processes in place to prevent misuse of their GTs, and respond appropriately when misuse is reported, this should further reduce the degree and risk of harm to UK / international citizens from GT misuse. It should also support the effective functioning of the UK telecommunications sector by reducing the frequency of security incidents and make it clear that number range holders are accountable for their use of GTs.

1.25 When deciding whether to open an investigation into a number range holder relating to misuse of their GTs, and if so the type of action that may be appropriate, we expect to take this Guidance into account.

1.26 The steps set out and the examples presented in this Guidance are not exhaustive. We expect the Guidance to be considered as a framework for how we might interpret the steps range holders are expected to take, depending on the services provided and the potential for malicious signalling to be generated. We expect range holders to take the steps that are reasonable and proportionate for their particular circumstances.

1.27 In using this Guidance, range holders will need to ensure they comply with their obligations under relevant data protection legislation and the Investigatory Powers Act 2016.

Who the Guidance applies to

1.28 This Guidance applies to number range holders that are providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling.

1.29 In this Guidance, we use the phrases number range holder / range holder to refer to both:

a) Operators that are a “Communications Provider” within the scope of GC B1 as defined in the GCs as meaning “a person who (within the meaning of section 32(4) of the Act) provides an electronic communications network or an electronic communications service”.
b) Other operators who have access to GTs through their number allocations which, for whatever reason, may not be considered a “Communications Provider” within the scope of GC B1 in a specific context but which are within the scope of Non-Provider Condition 2.4.

1.30 References to number range holders in this Guidance are references to UK number range holders and do not therefore include references to number range holders in the Crown Dependencies.

1.31 Where this Guidance refers to number range holders providing a service to a customer, a customer includes other communications providers, businesses or other persons who make associated facilities[7] available for the provision of a network or services and have the potential to generate malicious activity.

1.32 Residential or business customers that are the end users of conventional mobile services are not within the scope of this Guidance to the extent they cannot use SS7 signalling to undertake harmful activities as outlined in this Guidance.

1.33 Services provided by number range holders that fall within scope of the Guidance include services that rely on a GT and which provide access to signalling functionality. An example is translation services, such as GT modification, which could be used as an alternative arrangement by a range holder that previously leased its GTs to another party. GT modification allows a customer to send signalling messages indirectly via a number range holder's GT. While there are established applications for GT modification such as outbound roaming services, this type of service has the potential to generate malicious signalling because the customer has the capability to send signalling messages from the number range holder's GT.

1.34 Another example of services that have the potential to generate malicious signalling and are therefore within the scope of this Guidance are Home Location Register (HLR) lookup services. We discuss both GT modification and HLR lookup services further below.

1.35 Ofcom expects range holders to remain alert to the risks associated with such services and take appropriate steps to ensure their GTs are being used by their customers to provide legitimate services, in turn protecting UK / international citizens.

[7] See section 32(3) of the Communications Act 2003.

2. Guidance to prevent Global Title misuse

2.1 Where a range holder is providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling, we expect the range holder to take appropriate steps to prevent the misuse.

2.2 The nature and extent of the steps range holders will be expected to take will depend on what is considered appropriate in the specific circumstances, taking into account:

a) the nature of the service it is providing (and whether it should be considered higher risk);
b) the risk of malicious signalling;[8]
c) the customer the range holder is providing the service to;
d) knowledge of any previous malicious signalling carried out by that customer; and
e) that customer's intended use of the service.

2.3 All range holders should therefore first assess whether a particular service they are providing to a customer (using a GT as an input) has the potential to generate malicious signalling.

2.4 Where a range holder identifies a service that has the potential to generate malicious signalling, they are expected to, at minimum, take reasonable steps to understand the customer that has requested the service, and the risk of misuse, before providing the service. This includes Know Your Customer (KYC) checks, checks on the intended use of the service and considering any indicators of a high-risk customer.

2.5 As part of their assessment, range holders are expected to check for any unusual activity involving the customer's services. They should also ask 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.

2.6 Range holders are expected to record the steps that have been taken and ensure they are signed off by an appropriate senior manager.

2.7 Depending on the circumstances and the nature of the risk involved, range holders may also be expected to:

a) Put processes in place to ensure continued compliance with relevant numbering rules and prevent illegitimate use. This includes:

- putting appropriate contractual controls in place in relation to the use of the relevant service and to ensure customers are required to comply with relevant numbering rules;
- keeping risk assessments under review and updating them in response to significant changes to the commercial relationship between the range holder and the customer; and

[8] We expect range holders to have regard to the use of abnormal signalling traffic types identified in the GSMA's FS.11 publication - SS7 Interconnect Security Monitoring and Firewall Guidelines.

- routinely testing and/or monitoring specific risks associated with a particular customer

b) Put processes in place to appropriately respond to any incident where a customer is using a service (which uses the range holder's GT as an input) for an illegitimate purpose. This includes:
   - developing and maintaining a process for capturing and handling complaints and maintaining a record of any investigations, outcomes and action taken;
   - taking appropriate action to investigate and resolve incidents of potential illegitimate use in a timely manner; and
   - as far as reasonably possible, preventing any further potential illegitimate use once they have been informed of, or have identified, a potential concern. This may include requiring urgent action from the customer in response to a complaint, applying temporary blocks to services, or using contractual controls to withdraw services.

Services that are at a higher risk of generating malicious signalling

2.8 When assessing what steps are appropriate for a particular service, range holders should have regard to, among other things, the types of malicious signalling that may occur and the level of risk of that malicious signalling occurring.

2.9 Where a service with a higher risk of malicious signalling is provided, it is likely to be appropriate to include the steps described in paragraph 2.7, in addition to those in paragraphs 2.4 - 2.6 of this Guidance.

2.10 We have set out examples below of two types of service with a higher risk of malicious signalling and provide examples of measures that are likely to be appropriate to address the specific risks associated with those services.

Example 1: GT modification services

2.11 GT modification is an established alternative arrangement to GT leasing (e.g. it is associated with outbound roaming services). We are mindful that it might be considered for other services as a result of our ban on GT leasing.

2.12 GT modification services allow a customer to use a range holder's GT indirectly to exchange SS7 signalling messages with other mobile networks. While GT modification can reduce the risk of harm relative to GT leasing and enhance the transparency and accountability of the operators using GTs, we consider that there is still a significant risk of malicious signalling where services are provided using GT modification because the customer has the capability to send signalling messages. We would therefore encourage range holders and other operators to consider if there are alternative, lower risk methods available to facilitate the provision of mobile services.

2.13 If range holders consider it necessary to provide GT modification services then they are expected to implement further measures that are appropriate for these higher risk services, which is likely to include those identified in paragraph 2.7 above.

2.14 Taking into account the measures identified in paragraph 2.7 above, examples of more specific controls that it is likely to be appropriate for a range holder offering GT modification services to put in place include:

a) performing routine due diligence checks on customers to ensure GT modification is only facilitating legitimate services;[9]
b) implementing contractual measures that limit the customer's signalling to the specified service; and
c) carrying out routine monitoring and inspection of the customer's traffic via the range holder's firewall.

Example 2: Home location register (HLR) lookup services

2.15 A range of services are referred to as HLR lookup, including authentication services, least cost routing and number authentication services.

2.16 HLR lookup services are an example of a higher risk service because they facilitate access to operational data held by mobile networks, some of which may be personal data and/or location data which is subject to legal requirements under relevant data protection legislation.

2.17 We expect range holders providing, or indirectly facilitating provision of, HLR lookup services to be alert to the risk that such services may be facilitating access to operational data held by mobile networks which may be contrary to relevant data protection legislation.

2.18 Range holders directly providing or indirectly facilitating their customer's provision of an HLR lookup service are therefore expected to implement further measures that are appropriate for these higher risk services, which is likely to include those identified in paragraph 2.7 above.

2.19 Taking into account the measures identified in paragraph 2.7 above, examples of more specific measures that it is likely to be appropriate for a range holder to put in place include carrying out due diligence checks to:

a) determine whether data gathered by its customer is subject to data protection legislation, including the United Kingdom General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended; and
b) where applicable, ensure their customer is taking appropriate steps to comply with relevant data protection legislation, including but not limited to carrying out due diligence on customers to ensure that they:
   - have a legitimate basis for processing data; and
   - are complying with the requirements relating to the processing of location data in Regulation 14 of the Privacy and Electronic Communications (EC Directive) Regulations 2003.[10]

[9] For example, legitimate uses of GTs could include operators facilitating customers' ability to roam abroad.
[10] Where applicable, we expect range holders and their customers, to take appropriate steps to ensure compliance with the relevant domestic legislation in the country they are operating from.