An Coimisiún um
**Rialáil Cumarsáide**
Commission for
**Communications Regulation**

# Nuisance Communications
## Scam Calls and Texts

## Best Practice Guide for Businesses & Organisations

**Information Notice**

**Reference:** ComReg 23/01

**Version:** 1.0

**Date:** 13/01/2023

**An Coimisiún um Rialáil Cumarsáide**
**Commission for Communications Regulation**
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

# Content

# 1 Background

1) Nuisance Communications are unwanted, unsolicited communications generally directed at large portions of the population. Nuisance communications have the intent to mislead the receiver, so they unknowingly provide sensitive personal information. This in turn can enable criminals to perpetrate fraud.

2) This publication focusses on best practices for **businesses & organisations** and will help you identify genuine messages and protect your customers from scams.

3) ComReg has previously undertaken several other related initiatives:

- In 2004, to tackle the persistent problem of robocalling, direct dialling facilities to 13 countries, mainly in the South Pacific, were suspended[1].
- In 2012 – 2013, ComReg worked with the Data Protection Commissioner ("DPC") to address calls from a US group flooding Ireland with calls in respect of a referendum issue[2].
- In 2021 ComReg established the Nuisance Communications Industry Taskforce ("NCIT"[3]) to provide a co-ordinated approach by the Irish telecoms operators to combat this menace.
- 2022 saw the publication of the progress report on the NCITs activities[4] and the launch of its first anti Nuisance Communications initiative[5].

4) ComReg provides advice to consumers which is published on our website under our "Advice and Information" section[6]. Consumer news, posts and tweets are published as circumstances arise[7] [8] [9] [10] [11] [12]. ComReg regularly engages with stakeholders including our Consumer Advisory Panel[13], Age Friendly Ireland[14] and the Data Protection Commission, who have published their own guidance document for organisations on phishing[15].

---

[1] ComReg PR240904 - Statement by the Commission for Communications Regulation on measures to combat rogue auto-dialler programs | Commission for Communications Regulation (comreg.ie)
[2] Public hit by fresh spate of abortion 'robo-calls' - Independent.ie
[3] ComReg Document 21/129: Nuisance Communications – Formation of the Nuisance Communications Industry Taskforce
[4] IN 22/77: Nuisance Communications – Update on the Nuisance Communications Industry Taskforce
[5] ComReg Document 22/86: Nuisance Communications – Launch of 'Do Not Originate' Protocol
[6] https://www.comreg.ie/advice-information/scam-calls/
[7] https://www.comreg.ie/scam-calls-comreg-issues-a-reminder-to-consumers-to-be-vigilant/
[8] https://www.comreg.ie/scam-calls-comreg-warns-consumers-of-the-latest-scam-calls/
[9] https://www.comreg.ie/scam-calls-comreg-issues-a-reminder-to-consumers-to-be-vigilant-2/
[10] https://www.comreg.ie/scam-calls-comreg-advises-consumers-to-be-vigilant/
[11] https://www.comreg.ie/advisory-sms-scam-campaign-targeting-android-users/
[12] https://www.comreg.ie/smishing-warning-sms-scam/
[13] See Consumer Advisory Panel | Commission for Communications Regulation (comreg.ie)
[14] See Main – Age Friendly Ireland
[15] Guidance for Organisations on Phishing and Social Engineering Attacks

# 2 Introduction

5) Combatting telephone and SMS fraud requires a **collective effort**, everyone has a role to play. This guide focuses on **businesses and organisations**, and where they can help in the fight against nuisance communications, including fraud, through:
    a. Informed procurement processes; and
    b. Communications strategies.

6) The goal is to help you **protect your customers from fraud**, while also ensuring your telephone and SMS messages are consistent and trustworthy, reaching your target audience without being blocked or deleted as suspicious.

7) The practices outlined in this guide will **make it harder for criminals to exploit your communications** channels and by minimising complexity, enable greater focus and efficiency in detecting and preventing telecoms related fraud.

8) By following the guidelines and suggestions in this document you can make your organisation's telephone and SMS messages **more effective and trustworthy**.

# 3 Issues with Telecommunications

9) For most organisations, telephone and SMS messages represent an efficient and cost effective means of mass communication. These are essential tools for many organisations, particularly those that deal directly with the public.

10) Unfortunately, the technology and systems that underpin mass communications cannot always tell the recipient who originated a phone call or SMS message. This means criminals can pose as legitimate organisations, mimicking their communications very effectively, hiding within them a malicious link or a request for information or action by the recipient that enables fraud.

11) It is critical that legitimate businesses and organisations follow some basic guidelines, helping their customers to distinguish between genuine communications and fraudulent communications targeted on deception.

# 4 Creating Trustworthy Communications

12) To be recognised as legitimate, it is essential that your content meets the standards expected for your communications by your customers. Poor formatting, spelling mistakes and other inconsistencies are often hallmarks of fake communications.

13) When creating content for customer communications, please keep the following in mind:

- Do not request personal details;
- Do not include weblinks in SMS messages;
- If it is necessary to include weblinks, make sure they are human readable and easy to remember – do not use URL shortening services;
- Consistency in language and formatting is important across all your channels; and
- Avoid language that encourages panic or suggests urgency.

14) Speak with a single voice. You should keep the amount of telephone numbers, email addresses, and SMS Sender IDs[16] to an absolute minimum and ensure your messaging is consistent[17]. It is particularly important in larger organisations that all functions, including those involved in advertising, are aware of each other and their communications activities.

15) Consistency in your communications helps us all:

- **Make it simple**: if your messages come from a single, well-known source, it is simpler for recipients – your customers, to distinguish between legitimate and fraudulent messages.
- **Less is more**: fewer communications channels can be better protected, making them harder for criminals to abuse.
- **Help your customer recognise it's you**: make available easy to understand information explaining your communications process for your customers – include the kinds of information you would never ask. This will help you protect your customers from fraud, while ensuring your telephone and SMS messages are consistent and trustworthy.

[16] Refer to section 6 Contact by SMS

[17] Having a company-wide communications 'style guide' and/or policy will go a long way towards ensuring consistency.

16) If your organisation has phone numbers that are never used for making calls, then consider ComReg's free 'Do Not Originate' protocol[18]. ComReg has compiled a list of these numbers and has requested telecoms operators to block calls that pretend to originate from them.

# 5 Contact by Phone

17) Spoofing a phone number is easy for criminals. For example, they can make a call that begins in Asia and reaches you via Eastern Europe look like a local call from a number you trust.

18) To detect this deception, telecom companies rely on underlying data about the call, known as 'signalling information'. Unfortunately, this signalling information is not always applied accurately by all operators. This makes detecting spoof calls difficult.

19) Less is more – it is therefore essential that numbers used to contact customers be kept to a minimum, do not vary, and are well publicised. The work of preventing spoof numbers will then be more focussed and efficient.

20) You should also try to ensure that service providers are not routing your local or national calls overseas. Fraudsters will often attempt to originate calls with a spoofed Irish number from outside Ireland. Because of this, calls that have been routed overseas may be blocked, even if they are legitimate.

21) Before putting services in place you should know the answers to the following questions:

- What type of number(s) are you planning to use – shortcode[19], geographic[20], non-geographic[21] or mobile, etc.?
- Will all the calls be outbound-only or do you want to accept inbound calls as well?

[18] This consists of large volume phone numbers that consumers call for information (e.g., a call centre) or to report an issue (e.g., credit card problem). These are "inbound-only" phone numbers as they are only intended for inbound calls to an organisation. The numbers are never used for making calls to consumers. For further information see ComReg Document 22/86, available at the following link https://www.comreg.ie/publication/nuisance-communications-launch-of-do-not-originate-protocol

[19] See paragraph 23

[20] For example, numbers which begin with Irish area codes such as 01, 021, 056 etc.

[21] For example 0818 or 1800 in Ireland.

- Are you expecting to send or receive SMS? SenderIDs[22] and some numbers cannot receive messages.
- Who provides and maintains your IVR[23] system or call centre, including its location?
- Which phone provider assigned the telephone number?

22) Suggested telephone guidance you should follow:

- **Maintain consistency** on numbers used for services.
- **Provide clear mechanisms for customers to establish contact.** It's preferable to allow the customer initiate contact when providing personal information, as this significantly hinders fraudsters. This can be achieved through several channels, including email, online, or inbound calls.
- **Understand who is providing your telephony services and the routes they use.** Having fewer providers makes it easier to ensure, for example, that your calls are not being routed overseas.
- **Any service that only receives calls** should be added to the *Do Not Originate ("DNO")* list. This helps prevent the number from being used to make outbound calls. You should also make it clear that your customers will never receive a legitimate call from this number. For details on the DNO service see ComReg Information Notice IN 22/86, Guidance document for Organisations and Application form IN 22/86a and the ComReg webpage on DNO at www.comreg.ie/dno .
- **Check your provider is correctly identifying, or 'signalling' the numbers they use to make calls on your behalf.** Ensure your provider is authorised by a ComReg General Authorisation[24] and that they are following the ComReg Numbering Conditions of Use and Application Process document ComReg 15/136R3.
- **Confirm the routing for your calls does not go offshore.** Many fraudulent calls originate outside Ireland. Routing legitimate calls outside Ireland and back for a monetary saving makes it harder to protect your customers and can therefore prove more costly for you and your customers.

[22] The textual address that appears in place of the sending telephone number.
[23] Interactive Voice Response. This is a commonly used automated telephone system that combines pre-recorded messages or text-to-speech technology with a dual-tone multi-frequency (DTMF) interface to engage callers, allowing them to provide and access information without a live agent.
[24] See https://www.comreg.ie/industry/licensing/general-authorisation/

# 6 Contact by SMS

23) Careful consideration needs to be given to the purpose of your message and the details that you present as the originator of that message.

- **SenderIDs** (the textual address that appears in place of the sending telephone number) are aimed at building trust in messaging but unfortunately are not supported globally. They are case sensitive and are only designed for one way, business to consumer communication. These are sometimes referred to as “Alphanumeric Originating Addresses”, “Alpha Tags” or similar.
- **Shortcodes** are five digit numbers, beginning with 5, that generally need to be setup on the individual mobile networks, but can be setup to support 2-way messaging with Irish mobile customers.
- **Long dial/mobile numbers** can look like a person-to-person message.


Figure 1. Example of real and scam SMS with SenderID

24) Before putting any services in place you should know the answers to the following questions:

- Do you plan to use SMS at all? If so, who is the supplier?
- Does the service need 2-way communication?
- What SenderID, if any, do you propose to use? (SenderID does not support 2-way SMS)
- Are you planning to include weblinks and is that wise?
- Are you planning a bulk SMS campaign?
- Is the message price lower than market rates or too good to be true? If it is, the supplier/aggregator may be using 'grey routes'[25] which can result in a customer data compromise.

25) You should make sure that SMS suppliers (also known as aggregators) are required to tell you when they change provider and give you adequate notice of this change. When using a shortcode, you should make sure it is only used for your messaging purposes and not shared with other businesses or organisations.

26) You should try to work with an SMS service provider who is as close to the mobile telecom operators as possible. The more service providers between you and the telecom operator, the more can go wrong, including the loss or manipulation of customer data. It also becomes harder to investigate or stop any problems.

27) If you cannot find information on the SMS service providers website, ask them directly. If they won't or can't answer, there are probably grounds for concern.

28) Care should be taken when selecting your SenderID. It can often be difficult to differentiate between certain characters (for example the letter 'O' can look like the number zero '0') especially on a small screen. This is often exploited by criminals who use 'similar looking' SenderIDs.

29) Suggested best practices you should follow:

- **Try not to include weblinks in messages**. Where this is absolutely necessary, we recommend using simple, trusted links. You should not use URL shortening services.

[25] The term "grey route" is used to describe any route for SMS traffic which is not carried by the Short Message Service Centre (SMSC) of the terminating mobile operator. Such messages are generally subject to a lower level of visibility and control than messages sent over supported routes.

- **Understand your communications supply chain** – using fewer providers makes this easier to manage
- **If weblinks are absolutely necessary, ensure they are consistent in ALL messaging**, making it easier for people to check them independently.
- **Be careful when choosing a SenderID**. Keep the number of SenderIDs you use to a minimum and avoid special characters.
- **Audit your messages** – validate that the messages are received exactly as you sent them. Any changes to the content or message sender are indicators that your message provider is using grey routes, putting your messages at risk of fraud, delay, or even regulatory breach.

# 7 Best practice – ComReg's Top Tips

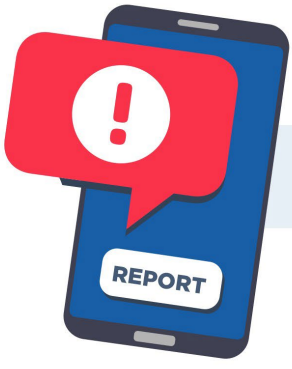
## A best practice guide for businesses

Commission for Communications Regulation
An Coimisiún um Rialáil Cumarsáide

### Protect your customers from scam messages


**These tips will help your customers identify genuine messages from you. They will also help reduce fraud on telecoms networks.**

1. Keep messages to your customers simple, clear and consistent.
2. Minimise the amount of phone numbers, SenderIDs and email addresses you use to contact customers.
3. Do not ask for customers' personal details by text or email.
4. Publicise your contact details, ensure your website describes how you contact customers (e.g. phone, email, SMS SenderID) and explain how your customers can verify communications from you.




5. Make sure everyone in your supply chain is aware of and applies the information in this guide.
6. Communicate clearly to your customers how they can report scams.
7. Use hyperlinks in text messages sparingly, ensuring URLs are easy to read and understand.


8. Consider using ComReg's 'Do Not Originate' service for your inbound only phone numbers. For details see **www.comreg.ie/dno**

For additional information for you and your customers visit:
**www.comreg.ie/advice-information/scam-calls/**