



Combating Scam Calls An Ofcom Perspective 2025

NICC Open Forum 2025

Jill Faure

Tim Gilfedder

12 November 2025



Agenda

Developments in the landscape of scam calls and messages

Ofcom's recent activities and interventions

Current focus of work

Looking ahead

Scams and fraud continue to affect UK citizens and consumers



I was fooled into paying £500 to be a model. Here's how to avoid my mistake



Judy attended two phoney photoshoots and paid a total of £500 for 15 photos

Yasmin Rufo
BBC News

7 October 2025, 09:02 BST

When 79-year-old Judy Corker from Manchester saw a social media advert calling for older models, it sounded harmless enough and the idea of getting glammed up and maybe earning a bit of money on the side was appealing.

"It said there was a lack of mature models, so I thought I'd fill in the form for fun," she tells BBC's Morning Live.

Over 1.8 million over-65s scammed online in the past year as Virgin Media O2 reveals new 'Scam Schools' programme

research from Virgin Media O2 reveals over-65s falling victim to social fraud lose £831 on average, with Brits left fearful of scammers targeting banks, HMRC and delivery firms.

More than half (55%) of Brits worry older loved ones could lose their life savings to fraud, with 39% doubting they'd be able to spot a scam.

As part of Get Online Week, Virgin Media O2 and Good Things Foundation are launching a free Scam Schools programme with sessions across the UK to help Brits get safer online.

Research from Virgin Media O2 reveals more than 1.8 million* over-65s have been scammed online in the past year, with the average victim losing £831**. A half (55%) of Brits fear their older relatives could lose their life savings to scammers, with almost four in ten (39%) not confident that they could spot a scam.

Share article



Media enquiries

Download logo

Subscribe for Alert
Full name



Children's names, pictures and addresses stolen in nursery chain hack



Joe Tidy
Cyber correspondent, BBC World Service
25 September 2025

Hackers say they have stolen the pictures, names and addresses of around 8,000 children from the Kido nursery chain.

The gang of cyber criminals is using the highly sensitive information to demand a ransom from the company, which has 18 sites in and around London, with more in the US and India.

The criminals say they also have information about the children's parents and

Outsourcing firm Capita fined £14m after millions had data stolen



Imran Rahman-Jones
Technology reporter

15 October 2025

16% of authorised push payment fraud cases were enabled by telecoms services in 2024 and £1.17 billion was lost to fraud in 2024 (UK Finance, 2025 [Annual Fraud Report 2025](#))

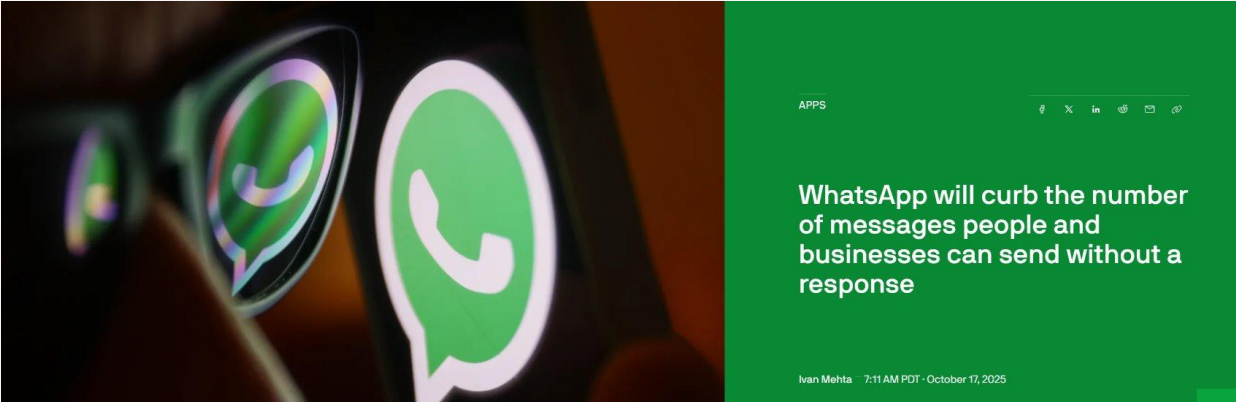
In February 2025, 42% of phone users (landline and/or mobile) reported that they had received a suspicious call in the last three months and about half of mobile users (51%) claimed to have received a suspicious mobile message in the last three months and about a third (32%) said they had received suspicious messages at least weekly (Ofcom 2025, [Experiences of suspicious calls, texts and app messages](#))

But law enforcement, public bodies and industry are fighting back...

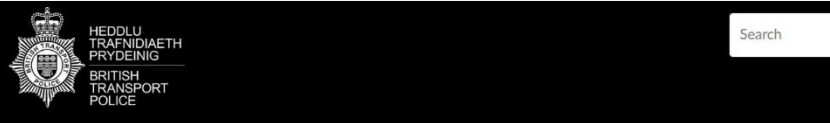
Press release

UK and US take joint action to disrupt major online fraud network

Alongside the US Government, the UK has today sanctioned a network that operates illegal scam centres across Southeast Asia.



TAKE FIVE TO STOP FRAUD



Report Tell us about Apply or register Request Thanks and complaints

Home > News

Man jailed for spamming commuters with phishing attempts - London

[England](#)
[In the courts](#)

Published: 16:05 16/10/2025

A man who used an SMS blaster to spam commuters with fraudulent text messages during rush hour has been jailed, following a British Transport Police (BTP) investigation.

Number spoofing scams

Published: 16 January 2023

There has been a recent increase in reports of 'number spoofing'. This is when scammers change their caller ID to disguise their identity from the person they are calling.



Police uncover 40,000 SIM cards linked to €5 million cyber scam across Europe

Ofcom has been active in scam prevention and mitigation

Combating scam calls involves working with:

Industry and industry groups

Regulators and government departments

Law enforcement agencies

Regulatory counterparts around the world



Home Office



Ofcom has also conducted more formal interventions over the past few years

The introduction and maintenance of the 'Do Not Originate' ([DNO](#)) list

Helping CPs block numbers associated with banks and government departments etc. that are never intended to make outbound calls

[Clarifying](#) the type of due diligence that UK providers should carry out when suballocating numbers to other CPs

Taking [steps](#) to significantly reduce malicious signalling from UK Global Titles, thereby providing material benefits to UK and international citizens

[Setting out](#) the steps that providers are expected to take to identify calls from abroad that are spoofing UK landline numbers and to block them

As a result of these (and other) interventions, we believe that major providers are blocking 1.2m calls a day as a result of these rules, perhaps as much as 1% of all incoming calls

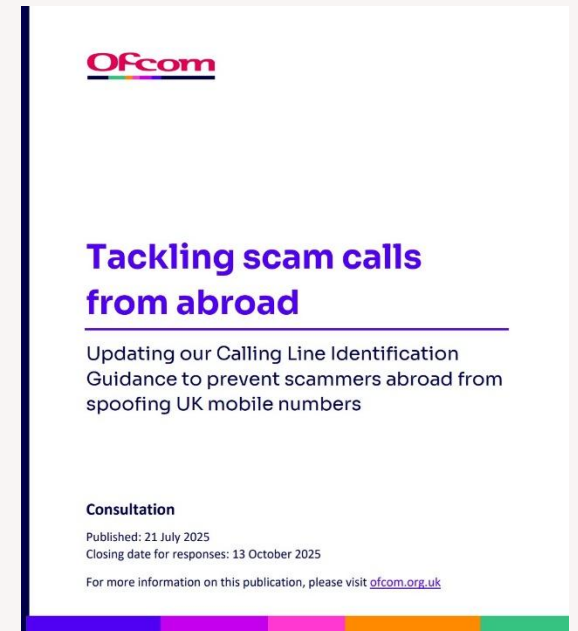
Earlier this year we consulted on proposals to combat scams calls spoofing UK mobile numbers

We are [proposing](#) to amend our CLI Guidance to set out how we expect providers to process calls from abroad that appear to come from UK mobile (+447) numbers

When these calls first reach a UK provider (including entities acting as international gateways), the provider should modify the call's CLI data to mark the CLI Presentation Number as 'withheld'

The deadline for responses has passed and we are now reviewing and considering our next steps

We plan to publish our final decision in early 2026



We have also just launched a consultation on combating scam messages

Our research shows that people are now more likely to have received a suspicious text message than phone call in the past three months

We have just published a consultation with [proposals](#) including Person to Person (P2P) and Application to Person (A2P) messages

For P2P messages we are proposing new General Conditions (GCs) to require mobile operators to prevent scam messages by:

- Setting volume limits for pay-as-you-go (PAYG) SIM cards
- Blocking numbers used by scammers
- Blocking scam messages in transit

For A2P messages we are proposing new GCs on mobile operators and aggregators to:

- Conduct due diligence (Know Your Customer checks)
- Prevent the use of fake alphanumeric sender IDs
- Conduct ongoing Know Your Traffic checks
- Apply incident management processes to block message senders
- Block scam messages in transit

We are also proposing new GCs for all mobile operators and aggregators to ensure these requirements are effective and to minimise the risk that providers block legitimate messages (such as rights to challenge and data protection processes)

The deadline for consultation responses is 28 January 2026

The Ofcom logo, featuring the word "Ofcom" in a bold, sans-serif font with a horizontal line underneath.

Combating mobile messaging scams

Proposals for new rules and guidance

Consultation

Published 29 October 2025

Closing date for responses: 28 January 2026

For more information on this publication, please visit [ofcom.org.uk](https://www.ofcom.org.uk)

A decorative horizontal bar at the bottom of the page, consisting of five colored segments: blue, purple, pink, orange, and green.

We are also reviewing the 'DNO' list

We are looking at migration of, and improvements to, the **Do Not Originate** list

- The DNO list contains 14k numbers and is shared with around 60 organisations
- We are making some process improvements for DNO updates, to introduce more automation in managing the list
 - The new process should be ready very soon
- We will contact DNO users ahead of this migration to update on the new process

The Do Not Originate (DNO) list

Published: 23 February 2022
Last updated: 16 March 2023

What is the Do Not Originate (DNO) list?

Consumers may be more likely to trust a call coming from a number associated with a known organisation. In some cases, scammers may deliberately change their number to hide their identity or mimic the number of a legitimate business, e.g. a bank, in order to mislead the consumer. This is known as 'spoofing'.

Some telephone numbers that are assigned to a business or organisation may never be used by that organisation to make outgoing calls. This may be the case where the number is reserved for inbound calls only e.g. the number on a bank card which is reserved for consumers to report problems to their bank. Any outgoing calls appearing to originate from these numbers will have been spoofed and will not be a genuine call from the organisation.

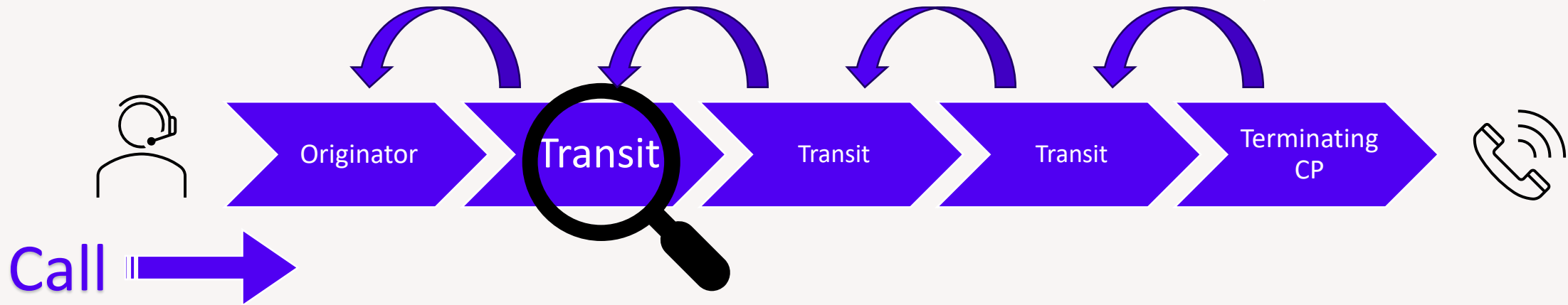
Ofcom and UK Finance set up the DNO list in 2019 and worked with telecoms companies, devolved administrations, government agencies such as HMRC and other public sector bodies, to record inbound-only telephone numbers that would not be used to call consumers.

The DNO list is shared with telecoms providers (and their intermediaries) to help them identify and block calls from numbers which are not used for outbound calls. We also share the list with some call blocking and filtering services. These services use technology to block or filter unwanted and nuisance calls on behalf of the consumer, for example via an app or hardware that is installed on a fixed line.

The list has been shown to be an effective tool in combating scam calls using spoofed numbers. For example, [HMRC reported a significant reduction in spoof calls](#) as a result of its inbound-only numbers being added to the DNO list. It should be noted, however, that adding a number to the list is not a guarantee that all calls will be blocked. Currently, not all providers apply the DNO list. Further, where providers are using the list, technical telephony constraints may mean that a small number of calls are still connected.

Adding numbers to the list

Traceback ? ? ? ? ← Traceback



Traceback is a recognised part of our approach to combat scam calls.

There is an industry commitment in the Government's [Fraud Sector Charter](#) to introduce a traceback process

We are reviewing how we would use the information obtained through traceback

This work includes review of:

- The technical process to be adopted (the focus of current NICC work)

- The information we would like to receive

- How we could use this information to help our functions to combat scam calls

We also participate in, and contribute to, international activities examining Traceback such as GIRAF

Looking ahead

How we may see Scam calls adapting to our measures

- Pure International CLI – particularly those resembling UK numbers

- PAY-GO (unregistered) Mobile numbers – no need to spoof

The role of Cloud based and OTT Voice services

Arms race in A.I. for scam call generation AND scam call mitigation

To complement our policy work we also have an active enforcement programme with respect to our existing rules

- Including two open investigations



Thank you / Contact details

Jill.Faure @ Ofcom.org.uk

Tim.Gilfedder @ Ofcom.org.uk