Tackling Scams, Fraud and Nuisance Calls

A Best Practice Guide for Magrathea Customers

Magrathea Telecommunications Ltd. Unit 5, Commerce park, Brunel Road, Theale, Berkshire RG7 4AB Tel: 0345 004 0040

Tackling Scams, Fraud and Nuisance Calls - A Best Practice Guide for Magrathea Customers

Scams, fraud, and nuisance calls are ongoing challenges across the telecoms sector. They continue to attract attention from both regulators and policymakers, and for good reason: the impact on end users can be serious.

There is no single fix, but applying a combination of proactive and reactive measures can significantly reduce the risks. These measures range from caller verification and call blocking, through to reporting incidents and taking steps to prevent repeat misuse.

This guide is designed to help you strengthen your monitoring processes so you have a clear picture of how your services are being used. By spotting unusual call patterns quickly, you can act to stop problems before they escalate - whether that means investigating further, applying call blocks, or suspending service where appropriate.

The guidance is deliberately broad so that providers of all sizes and service models can use and adapt them to their own operations. You should decide what measures are proportionate, effective, and compliant with Ofcom requirements for yourself, and ensure processes are documented.

This guide should be used alongside our other best practice resources, available via The Guide in the MAGIC Portal, to ensure a joined-up approach.

Know Your Traffic (KYT)

Understanding your voice traffic is essential for both compliance and operational success. You may already track call data for commercial reasons and often these same tools can be adapted to detect fraud or scams.

A useful starting point is to define a baseline: establish what “normal” traffic looks like for your network and customer base. This benchmark helps you quickly distinguish between safe and potentially risky activity.

High-risk traffic can be broadly categorised as:

- Hacked switchboards - where compromised equipment (such as PBXs) is used to generate unauthorised calls, typically to premium rate or high-cost destinations.
- Targeted scam calls – calls to make direct contact with a potential victim, usually as part of a wider social engineering campaign or fake advertising campaign response.
- Bulk scam or nuisance calls - calls designed to mislead or defraud often utilising current social weak points e.g., Accident Compensation or HMRC impersonation) but their calling patterns are usually recognisable, especially when combined with strong KYC (Know Your Customer) measures.

While hacked systems present technical and financial risks, this guidance focuses mainly on bulk scams and nuisance calls, where robust monitoring and prevention measures can make the biggest difference to reduce consumer harm.

Proactive Monitoring

Caller Line Identification (CLI) Screening:

CLI screening is a critical first step in tackling misuse. At Magrathea we screen CLIs as calls pass through our network, but we also require customers to apply their own checks before handing calls to us. Together, these layers of verification create stronger protection.

At a basic level, we validate CLIs for digit count, format, and allocation in line with the UK Numbering Plan.

Other things to consider:

- Call-back requirement - all presented CLIs should connect back to a working number with a clear caller identification (whether via a live answer or an IVR/recorded greeting).
- Overseas traffic - overseas-originated calls must not use a UK CLI, except in very limited, justifiable cases. We will block calls that do not meet this requirement, so if this is a requirement for you please contact us to discuss your specific business needs.
- Reporting – we recommend that you keep a record of calls blocked under CLI restrictions. This data often highlights emerging sources of nuisance calls and can inform future prevention measures.

Do Not Originate (DNO) List Screening

The Ofcom DNO list includes numbers that will never be used for outbound calls. Any call using one of these numbers is almost certainly spoofed and we will block such calls automatically and report them to you.

If your customer originates calls that trigger a DNO block, this should prompt further investigation into their calling practices and service use. In many cases it can be an early warning sign of misuse.

More information on Ofcom's DNO list can be found here.

Telephone Preference Service (TPS) Screening

The TPS allows individuals and businesses to opt out of unsolicited live sales and marketing calls.

If you screen customer traffic against the TPS register, watch for high block rates. These can point to poor list management or non-compliant marketing practices that may need closer review.

More information on the TPS and how to obtain a copy of the TPS list is available here.

Magrathea Telecommunications Ltd. Unit 5, Commerce park, Brunel Road, Theale, Berkshire RG7 4AB Tel: 0345 004 0040

Ongoing Monitoring Metrics

Scammers constantly adapt their methods, so monitoring needs to continuously evolve too. Below are some useful indicators to watch for. This list is in no way exhaustive and you may find others based on your own traffic baseline.

- Sudden changes in traffic levels - spikes or drops may indicate blocked traffic shifting from other networks.
- Short duration calls - large numbers of very brief calls may suggest nuisance activity.
- Answer Machine Detection (AMD) patterns - many sub-one-second calls or calls lasting just a few seconds should trigger review.
- Low Answer Seize Ratio (ASR) - conversational calls typically have an ASR of ~65% or higher. Significantly lower rates can indicate outdated or non-compliant calling lists.
- War-dialling - sequential number dialling may signal crude scam attempts.
- Hang-up cause analysis - a high rate of call terminations by recipients can indicate unwanted or intrusive calls.

Automated monitoring systems are vital, but having a human review by experienced staff is highly recommended as they often spot patterns or anomalies that machines miss. Never underestimate your team's gut feel!

Incident Handling and Misuse Response

All providers should have a clear, documented process for dealing with suspected misuse. This should cover:

- Reporting - how suspected incidents are raised internally and externally.
- Investigation – steps to review the issue and respond, with timescales proportionate to the severity of the incident.
- Evidence - keep traffic metrics, KYC data, complaints, warning lists - and any regulator or law enforcement input - to support your decisions.

Where misuse is confirmed and cannot be legitimately explained, take reasonable steps to prevent further abuse. Options include applying call blocks, suspending services, and/or invoking contractual terms.

Always support affected consumers where appropriate, cooperate with Ofcom and other relevant bodies, and – if applicable - notify range holders of issues involving sub-allocated numbers.

If criminal activity is suspected, contact law enforcement. You can also report via Report Fraud's online reporting service or by calling 0300 123 2040.

We also encourage you to report any suspicious activity to the National Trading Standards data-sharing scheme, established by Comms Council UK and the NTS in January 2025 to help strengthen the industry's collective defences against fraud. Further information about this scheme is available here.

Magrathea Telecommunications Ltd. Unit 5, Commerce park, Brunel Road, Theale, Berkshire RG7 4AB Tel: 0345 004 0040

A note on how we handle misuse:

If we detect an incidence of potential misuse of our numbering or services, we will contact you in the first instance for your input on this. Please make sure we have the correct contact information to get hold of you in and outside of office hours. If we cannot reach you or if there is irrevocable evidence of misuse, we do reserve the right to suspend part or all of the service provided to you in order to protect the integrity of the network and mitigate the potential for consumer harm. **Final Note:** By combining strong KYT monitoring, effective KYC processes, and a clear incident response plan, providers can protect their networks, their customers, and the wider public from the harm caused by scams and fraud. Magrathea is here to support you in that effort. More information and guidance on implementing effective KYC and due diligence best practice in the UK can be found in The Guide which is accessed via the MAGIC portal.

Magrathea Telecommunications Ltd. Unit 5, Commerce park, Brunel Road, Theale, Berkshire RG7 4AB Tel: 0345 004 0040