Magrathea Telecommunications Limited,
5 Commerce Park, Brunel Road, Theale,
Berkshire RG7 4AB

0345 004 0040 info@magrathea-telecom.co.uk

Guidance on compliance - originating calls to the USA

This document is for clarity and guidance but does not seek to replace official regulations or guidance and all Service Providers are responsible for satisfying themselves that they are adhering correctly to current standards and rules. Magrathea accepts no liability whatsoever for any errors, omissions or statements in this guidance or for any loss which may arise from your use of this guidance.

Who should make use of this guidance

Anyone terminating calls regularly to the USA needs to ensure that they are compliant with current rules and regulations. Even if your business cannot be held account under US Federal Law, the local carriers are being held to high standards and will block traffic and support legal action against any perpetrator of illegal traffic.

As any reputable carrier in the US will not want to be subject to fines or have their ability to carry calls restricted, they are likely to take a zero-tolerance approach to any overseas networks who might deliver them non-compliant traffic.

Whilst Magrathea's own monitoring and engagement with call profiles will capture many 'bad actors', we require each of our clients to take steps to ensure that illegal, nuisance and scam calls do not enter our network.

Key actions to take

- Check you have carried out recent and relevant due diligence on your customer
- Register with the FCCs Robocalls Mitigation Database and notify us of your FRN
- Inform your team how to deal with Traceback requests

Who sets the rules and regulations

The Code of Federal Regulation known Title 47 is essentially the US Law that relates to telecommunications in the US. The Code sets out the role of the Federal Communications Commission (FCC) and the rules they require around various use cases.

Like Ofcom in the UK, the FCC have a broad remit and the Code sets out a number of sub-chapters to explain the rules. Similar to the General Conditions of Entitlement we have in the UK.

In addition, in 2019 a new Act gave the FCC additional tools to fight unwanted robocalls – called the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence). Large fines, call authentication services and a new traceback system are amongst the tools that can now be used to clamp down on nuisance calls.

The tools you need to be aware of

STIR/SHAKEN

In June 2021, it was mandatory to implement STIR/SHAKEN within your network if you are originating calls in the US. Whilst each of our US carriers are required to comply, as a UK business we are not part of the STIR/SHAKEN initiative and therefore the carrier will attest only that they know where they have received the call from (Gateway Attestation C).

Robocall Mitigation Programme

All providers must register with the Robocalls Mitigation Database and receive an FCC Registration Number (FRN).[1] You must also commit to taking all reasonable steps to avoid originating illegal robocall traffic and they must commit to responding to Traceback requests (see below) within 24 hours.

When registering you need to upload a document to certify that all calls originated are subject to a robocall mitigation program, and in the case of any provider who hasn't adopted STIR/SHAKEN you must also declare this in the certificate. See the information at note 1 for full details of what to include in your certificate and visit here to setup an account to register: https://www.fcc.gov/licensing-databases/fcc-user-login. Once complete please notify Magrathea of your FRN for our records.

Important Note: US carriers will now only carry traffic if the originating service provider has registered in this database – please act immediately.

Traceback

The new TRACED Act required a consortium that would conduct the tracing of suspected illegal robocalls back to their originator. The Industry Traceback Group (ITG) was formed[2].

To enable each provider in the chain to pass on details and move another step closer to the source, a portal was created.

The Traceback Portal utilises the Robocall Mitigation Database, so when provider discovers where the call entered their network they can search for the provider who is next in the chain and the traceback request will be sent to them. This continues until the end of the chain is reached or a party is non-responsive.

If the provider is not in the Robocalls Mitigation Database, they will be noted as such and entered manually. This information is likely to cause others in the chain to block calls as all providers need to be in the database.

You do not need to register for the Traceback portal proactively, you can do so if/when you receive a complaint to respond on.

Important Note: If you do not respond within 24 hours you will start getting warnings against your name – it's important to make sure your team are ready to respond 7 days a week.

1. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-HH/section-64.6305
2. https://tracebacks.org/for-providers/