Maintel SIP
Acceptable Usage Policy

June 2020

1. Introduction

This document defines Maintel's accepted voice traffic profile, performance parameters for diallers and our governance for nuisance and malicious calls, for SIP endpoints connected to the Maintel Network.

Maintel reserves the right to limit or prevent traffic that breaches the guidelines in this policy or in the event any particular traffic presents a risk to the integrity of Maintel's network or product platforms. This policy is in line with standard Industry practice and other service providers involved in originating, transiting or terminating voice traffic may take similar action at their discretion.

In regards to nuisance and malicious calls there are two broad categories which are considered separately, however, both are as serious in their own right.

Unwanted marketing calls as well as Silent & Abandoned Calls are the first category, referred to as Nuisance Calls,

Malicious Calls, relating to calls with obscene content or that are deliberately designed to cause harm or offence. An extension of the latter is a deliberate denial of service attack on a call centre, colloquially referred to as a "Spam" over Internet Telephony ("SPIT") attack.

The scope of this policy are calls that, in some respect, transit Maintel's network.

2. Usage

- Maintel reserves the right to disconnect any end-point where usage is deemed illegitimate or excessive in terms of use.

- Calls exceeding any monthly allowance that has been agreed, or calls to numbers outside any call allowance that has been agreed will be charged at the call rates in the appropriate SIP rate card tariff.

3. Nuisance Calls

A Nuisance Call is one that is either unwanted or one that is "silent or abandoned" which means that a call centre is not following the regulations on availability of live operators etc.

Unwanted Calls

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), prohibits organisations from making unsolicited live or automated direct marketing calls to Subscribers (business or residential) who have registered their number with the Telephone Preference Service ("TPS"). PECR also prohibits organisations from sending unsolicited direct marketing emails or SMS text messages to individual subscribers who have not consented to receiving such messages and/or whom have previously explicitly told them they do not want them.

On 26th May 2011, the Information Commissioner's Office ("ICO") gained powers to serve third party information notices on communications providers and to impose civil monetary penalties of up to £500,000 for the most serious breaches of PECR. New statutory guidance was published on 30 January 2012 and a number of companies have already been fined.

Silent and Abandoned Calls

The Office of Communications ("Ofcom") is responsible for the enforcement of a silent or abandoned call. This is where a predictive dialler makes more outbound calls than the centre has agents for and the recipient gets dead air; or an abandoned call, which is where the ringing stops because the number of available agents has been used, as it has been deemed to be an offence (misuse of a public electronic communications network) under Section 127 of the Communications Act 2003 and has the power to fine up to £2m per offence. Section 127 offences also carry criminal liability. The exact rules are replicated herein under “Dialler Regulatory Standard”

4. Dialler and CLI Standards

Dialler Regulatory Standard

Diallers or any "automatic call generation" service connected to the Maintel Network, must comply with the following standards:

Ensuring an abandoned call rate (including a reasoned estimate of false positives) of no more than 3 per cent of live calls per campaign or per call centre over any 24 hour period;

Ensuring that people are not contacted within 72 hours of their receiving an abandoned call without the guaranteed presence of a live operator;

Playing an automated message in the event of an abandoned call telling the person called on whose behalf the call was made and providing them with a number to dial to stop any future marketing calls from that organisation;

Making valid and accurate calling-line identification ("CLI") information available to call recipients so they can identify who rang them via caller display or by dialling 1471 in the event of a silent call; and

Ensuring that where a call has been identified by dialler equipment as being picked up by an answer machine, any repeat calls to that specific number within the same 24 hour period are only made with the guaranteed presence of a live operator.

This Standard is a verbatim replication of the Ofcom guidelines5 and as such would be considered by Maintel to be a regulatory requirement to be adhered to by any signatory to our contracts.

Dialler Operational Standard

The Maintel Operational definition of Dialler Traffic is as follows:

This is traffic which typically has

- an Average Length of Call ("ALOC") of under 30 seconds with
- an Answer Seize Ratio ("ASR") less than 60%.

For clarity, this is the Maintel default position to ensure that we protect the network and all Maintel customers and exceptions can be considered by the Networks Director and Operations with an appropriate business case; however, any traffic outside of this profile will automatically have remedial action considered.

Operational Standard

Maintel reserve the right to limit (through call gapping or other operational intervention as we see fit in our sole discretion) which we feel may endanger the rest of the network. Any (but not limited to) of the following traffic patterns are not allowed:-

- Large amounts of call attempts hitting the same area or number type

No one geographic dialling code should exceed 5 CPS unless previously agreed. Large, unexpected and unmanaged spikes of traffic cause network monitoring fault alarms and should be avoided.

- Time of Day

Dialler traffic will be the first type to be shed during any network faults or high traffic periods.

- Call attempts to a large percentage of unallocated numbers.

ASRs below 40% will be deemed as suspect (e.g. Data cleansing activities) and would probably be a breach of the Regulatory Standard above. Immediate action will be taken to limit such traffic.

- Each endpoint will have a defined calls per second limit.

Typically customers are set to 5 CPS to begin with. Higher CPS can be negotiated on a case by case basis. Depending on the nature of the traffic bespoke solutions may need to be designed that may result in additional costs.

The endpoint must control their traffic within the agreed limits. Sending too many calls will get a 486 response and uses unnecessary SBC processor resource.

- General Maintel Network Alerts

Maintel has a large range of network performance alerts. For example a sustained low ASR being sent to one Mobile Operator type will produce and alarm in the Maintel NOC.

False alarms can hide other network problems and diverts resource away from projects and product development. Therefore if a Dialler pattern is thought be causing alarms or red statuses on the NOC monitors remedial action will be taken.

5. Dialler Removal Process

Daily reports are run to detect suspicious activity. The customer will be asked to stop sending this traffic but Maintel reserve the right to reduce their capacity or be turned off to protect the integrity of the network.

CLI Presentation

Maintel offers customers flexibility in what CLI they present . The Customer Agreement that has to be signed prior to implementation contains a condensation of the CLI Presentation regulations .

The two main points are:

- That the allocated entity for the number being presented has authorized its use for this purpose.
- The number being presented is not one to a revenue sharing number that generates an excessive call charge. That means you cannot present 09 or 118 and that 070/076 are likely to be in breach.

Periodic audits of presentation CLIs across the network will be performed and take action to enforce these rules as required.

Additionally, some operators within some countries within the European Economic Area (“EEA”) surcharge calls made from outside the EEA, and use the presentation and/or network CLI to differentiate. In the case of a malformed CLI, the default is to apply a surcharge which may be passed onto our customers. Care should be taken generally due to the rules, but should be especially taken when presenting a non-UK CLI.

6. Enterprise Contact Centre Solutions

Outbound Traffic Policy

This follows the standards outlined in the section under Dialler and CLI Standards.

Traffic which typically has an Average Length of Call ("ALOC") of under 30 seconds with an Answer Seize Ratio ("ASR") less than 60% is not generally acceptable. Inbound Traffic Policy

Large volume inbound campaigns may cause overload scenarios on the Maintel network and the

PSTN in general. In this traffic direction the calls per second limit on each endpoint is not active. If this traffic is causing network alarms then Maintel will invoke network call gapping across the network elements and may also request BT and other CPs to invoke call gapping on the inbound numbers causing the issue. Call gapping levels will be set at a level which protects the network. In some cases this may be to stop all calls to this number.

If a large volume inbound campaign is planned then it should to flagged to the Maintel NOC. This will allow planning on protective call gapping levels and allow special monitoring to be put in place.

There are processes across the industry for dealing with these events with communications between BT and the main CPs.

Carrier Pre Select Traffic Policy

This follows the standards outlined in the section under Dialler and CLI Standards. Generally the technology used from PBXs using CPS over Q931/ISDN30 hold back the potential for high calls per second levels. There is no per endpoint calls per second limit on single Carrier Pre Select CLIs. If traffic patterns are causing network alarms then calls from this CLI will be barred under the rules outlined under Dialler Policy.

Malicious Calls

These, like silent and abandoned calls, are also a Section 127 of the Communications Act 2003 offence and carry criminal liability. There are two broad categories;

- Spam over Internet Telephony ("SPIT") which is the telephony equivalent of a Distributed Denial of Service (DDOS) attack on a website.
- Calls intended to cause annoyance or offence.

Obviously, a SPIT attack can contain content that falls into the latter category too. Both need handling in a slightly different way.

SPIT Attack

Such an attack could compromise Maintel's network integrity, therefore it is expected that the appropriate operational teams will take whatever steps necessary to guarantee the integrity of the network as they would in a failure state; once mitigated, it should be treated as any other attempt to hack or misuse our network with appropriate investigation and involvement of law enforcement.

Where reports of these are made, they should be directed to the Network Operations Centre.