

FCC Robocall Mitigation Submission

Current Version	1.0
Status	Released
Date	24th May 2023

Author	Tony Friar
Department	Technology
E-mail	tony.friar@velonasystems.com
Telephone	+44 (0) 7887 843102

Document owner	Tony Friar
Department	Technology
E-mail	tony.friar@velonasystems.com
Telephone	+44 (0) 7887 843102

1 Table of Contents

1	TABLE OF CONTENTS	2
2	DOCUMENT CONTROL	3
2.1	DOCUMENT HISTORY AND STATUS	3
2.2	RELATED DOCUMENTATION	3
2.3	CONTRIBUTORS	3
2.4	DOCUMENT REVIEW TEAM.....	3
2.5	DISTRIBUTION LIST.....	3
3	ABOUT THIS DOCUMENT	4
3.1	PURPOSE OF THIS DOCUMENT	4
3.2	SCOPE OF THIS DOCUMENT	4
3.3	AUDIENCE.....	4
3.4	KNOWN ISSUES.....	4
4	INTRODUCTION	5
5	DESCRIPTION OF SERVICE.....	6
5.1	CALL DEFENDER	6
5.2	NO OUTGOING CALLS FROM END CUSTOMERS.....	6
6	PREVENTION & MANAGEMENT OF SERVICE ABUSE	7
6.1	PROACTIVE MANAGEMENT.....	7
6.1.1	The Nature of the Service	7
6.1.2	Compromised Core Network Nodes	7
6.1.3	Know Your Customer (KYC).....	7
6.2	REACTIVE MANAGEMENT	7
6.2.1	Fraud Management Systems	7
6.2.2	Co-operation with Traceback Requests	7
APPENDIX 1	LIST OF FIGURES	8
APPENDIX 2	LIST OF TABLES.....	9
APPENDIX 4	GLOSSARY.....	10

2 Document Control

2.1 Document History and Status

Version	Date Released	Issue/Amendment Details
1.0	24 th May 2023	First release

Table 1: Document History and Status

2.2 Related Documentation

Name	Version	Company	Department
Robocall Mitigation Database External Filing Instructions	December 2022	FCC	FCC
FS.38	1.0	GSMA	Fraud and Security Group

Table 2: Related documentation

2.3 Contributors

Name	Company	Department/Function
Tony Friar	Velona Systems Ltd	CTO
John Daly	Velona Systems Ltd	CEO

Table 3: Contributors

2.4 Document Review Team

Name	Company	Department/Function
Tony Friar	Velona Systems Ltd	CTO
John Daly	Velona Systems Ltd	CEO

Table 4: Document Review Team

2.5 Distribution List

Name	Company	Department/Function
FCC Mitigation Database	FCC	FCC Mitigation Database
John Daly	Velona Systems Ltd	CEO

Table 5: Distribution List

3 About this Document

3.1 Purpose of this Document

When registering in the FCC Robocall Mitigation Database, in relation to the STIR/SHAKEN section of the registration, if “Option 2” or “Option 3” is selected for “Voice Service Provider Certification” and / or “Gateway Provider Certification”, a document explaining the specific reasonable steps the Voice Service Provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program must be uploaded. This document has been produced to fulfil the requirement.

3.2 Scope of this Document

This document covers the requirements described above for the FCC Robocall Mitigation Database registration. This document does not cover areas other than those related to the registration.

3.3 Audience

This document is intended for upload to the FCC Robocall Mitigation Database.

3.4 Known Issues

There are no known issues with this document.

4 Introduction

Unsolicited calls, robocalls and fraudulent calls represent a serious threat to the telecommunication industry and its customers.

Velona Systems analyses and evaluates the risks facing the company and its business environment within the framework of the Velona Systems risk management system. Velona Systems complies with the relevant sections of the GSMA FS.38 SIP Network Security standard. Consequently, clear policies and procedures for overall prevention of service abuse framework have been defined.

5 Description of Service

This section describes the service offered by Velona Systems and how the service uses incoming and outgoing calls.

5.1 Call Defender

Velona Systems provides a Telephony Denial of Service (TDoS) defense solution for small to medium call centers. This solution is called Call Defender.

Call Defender protects call center customers from volumetric call flooding DoS attacks that arrive via the PSTN. Velona Systems provides Toll Free or geographic numbers to the call center customers and the customers advertise these numbers. Incoming calls to these numbers are analyzed by Call Defender and if all checks are passed, the calls are sent to the call center customer.

Some customers have direct SIP trunks to Call Defender, some customers register their SIP endpoints to Call Defender, and when neither of these connections is available or is not implemented, the calls are routed to the customer over the PSTN.

5.2 No Outgoing Calls from End Customers

Velona Systems does not provide an outgoing call service to our end customers. Call Defender will only ever initiate outgoing calls to the known numbers of Velona customers. As such customers cannot make Robocalls.

6 Prevention & Management of Service Abuse

This section describes the approach used by Velona Systems to prevent and manage service abuse.

6.1 Proactive Management

6.1.1 The Nature of the Service

The nature of the service offered by Velona Systems (end customers cannot make outgoing calls) makes it unlikely that our PSTN/PLMN connectivity could be used to initiate Robocalls.

6.1.2 Compromised Core Network Nodes

The main risk we see that would allow our service to be used to initiate Robocalls is a scenario in which one or more of our core network nodes was compromised. To negate this we comply with all relevant sections of the GSMA FS.38 SIP Network Security standard. We also utilize fraud management systems to detect any unauthorized usage.

6.1.3 Know Your Customer (KYC)

Even though the nature of the service makes it unlikely that the service offered by Velona Systems could be used to initiate Robocalls, Velona Systems performs extensive checks on new customers before they are provided with service.

6.2 Reactive Management

6.2.1 Fraud Management Systems

Velona Systems utilizes fraud management systems to detect any unauthorized usage.

6.2.2 Co-operation with Traceback Requests

Velona Systems will provide full co-operation with any traceback request.

Appendix 1 List of Figures

No table of figures entries found.

Appendix 2 List of Tables

Table 1: Document History and Status	3
Table 2: Related documentation	3
Table 3: Contributors	3
Table 4: Document Review Team	3
Table 5: Distribution List.....	3

Appendix 4 Glossary

Term	Definition
ACL	Access Control List
A-SBC	Access Session Border Controller
ATA	Analogue Terminal Adapter
BRI	Basic Rate Interface
CDR	Call Detail Record
CPE	Customer Premise Equipment
CPU	Central Processing Unit
E-SBC	Enterprise Session Border Controller
ISDN	Integrated Services Digital Network
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
HLD	High Level Design
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	IP Security
LLD	Low Level Design
LTE	Long Term Evolution
PoE	Power over Ethernet
PRI	Primary Rate Interface
QoS	Quality of Service
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SCP	Secure Copy
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Small Medium Enterprise
SRTCP	Secure Real Time Control Protocol
SRTP	Secure Real Time Protocol
SUT	System Under Test
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution