



CONSULTATION PAPER

Preventative measures to mitigate CLI spoofing and vishing scams

Consultation and Proposed Decisions

MCA Reference: MCA/C/23-5080

Publication Date: 29 September 2023

 (+356) 2133 6840  info@mca.org.mt  www.mca.org.mt


 Valletta Waterfront, Pinto Wharf, Floriana FRN1913, Malta

TABLE OF CONTENTS

1	Introduction.....	1
1.1	Context.....	1
1.2	Background	1
1.3	Scope.....	3
1.4	Definitions and Abbreviations	3
1.5	Legal Basis.....	6
2	Proposed Preventative Measures	7
2.1	High-level Principles	7
2.2	Types of Legitimate Calls	8
2.3	Preliminary Discussions	9
2.4	The Framework of Interventions	11
3	Performance Monitoring.....	22
4	Implementation Timeframes.....	23
5	Submission of Feedback.....	24
	Annex 1: Legitimate Call Types.....	25
	Annex 2: Candidate Measures in Preliminary Discussions.....	29

1 Introduction

1.1 Context

Scams which involve the spoofing of the Calling Line Identification (CLI) for calls and the Sender ID for SMS are on the rise globally, facilitated in their spread and evolution by advancements in online communications solutions. Scammers increasingly rely on spoofing of locally known numbers for voice calls (*vishing*) or of familiar SMS Sender IDs (*smishing*), to abuse of potential victims' knowledge of, and trust in, such numbers and identifiers.

Such 'social engineering fraud' scams¹ “*exploit a person's trust in order to obtain money directly or obtain confidential information to enable a subsequent crime*”. Such scams have a cross-industry effect with impacts that are simultaneously social, economic, and regulatory in nature: thus, multi-faceted solutions are a must.

From the perspective of the Malta Communications Authority (MCA), scams based on the misuse and/or unauthorised use of numbering resources and identifiers can understandably have a negative impact on subscribers' trust in such numbers and identifiers, and on the consumption of electronic communications services (ECS) in general. This Consultation Paper therefore presents some proposed decisions intended to mitigate this impact through measures introduced at an electronic communications network (ECN) level with the aim to contribute, in conjunction with other measures, towards the broader fight against such scams.

1.2 Background

Prior to the publication of this Consultation Paper, the MCA kept itself informed on salient developments in the field of ECS-based scams, particularly through desk research, participation in international fora, and discussions with local ECS providers and other stakeholders alike. Accordingly, it is evident to the MCA that scammers can nowadays leverage multiple ECS channels to target their victims, and that phone calls and SMS are among the channels most used for such scams.

It also emerged that the majority of scam calls are transited into the country from abroad, via operators of international network interfaces. This 'international dimension' to scam calls is a characteristic of scam communications across the globe and is therefore not exclusive to communications targeting Malta. It should be noted, however, that this characteristic adds an element of complexity in the fight against scams, since *illegitimate* calls invariably mix with *legitimate* calls received over international network interfaces, such as calls placed by outbound roamers terminating on national numbers, or calls with a national calling party number (CgPN) towards inbound roamers. Accurately determining legitimacy of incoming calls is thus key to the success or failure of any intervention.

It is recognised, however, that the task of distinguishing between legitimate and illegitimate calls is challenging, particularly given that malicious actors use the same, or very similar, tools that facilitate legitimate calls.

¹ Interpol, *Social Engineering Scams*. Accessible at <https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams>. Last accessed on 28 September 2023.

Against this context, a correspondingly global effort is underway to study and implement a wide range of (potential) solutions. Such solutions include, amongst others, measures to block calls through rule-based filters (e.g. calls where the CgPN is from specific numbering range(s), calls where the CgPN is “blacklisted”, or calls where the CgPN is clearly invalid or incomplete). Some solutions also propose the use of real-time checks (e.g. on roaming status) to detect possible spoofing of mobile numbers, whereas others consider the application of artificial intelligence (AI) to analyse traffic patterns for unusual activity which could be indicative of potentially fraudulent behaviour.

Since 2021, the MCA has engaged with locally authorised² undertakings who operate international network interfaces. In particular, the MCA sent out exploratory emails to these undertakings in order to seek industry input on ECS-based scams experienced in Malta which involve the spoofing of the CLI and/or SMS Sender IDs. These exchanges were also intended for the MCA to obtain initial insights on potential preventative measures that could be introduced at an ECN level to mitigate such scams and the capabilities within local operators’ networks to implement these measures. In view of the increasing prevalence of vishing and smishing scam attacks experienced in the first half of 2023, the MCA stepped up its activity in this area and, during the period June to September 2023, the MCA carried out preliminary discussions on potential preventative measures with locally authorised undertakings who operate international network interfaces. The MCA also set up an ad hoc steering committee, including participants from each of these operators, with the primary focus being for participants to provide preliminary feedback and recommendations on the practicability, implementation timeframes, costs and benefits of different potential preventative measures that may be considered to mitigate CLI spoofing, vishing and smishing.

At the time, the MCA expressed its preference that such preventative measures should be introduced in an incremental approach, in order to address the matter in a timelier manner. In this regard, the measures proposed were captured under three broad ‘Phases’, representative of potential phases of intervention, as follows:

- **Phase 1:** Measures to address incoming calls over international network interfaces with potentially spoofed national CgPN (except where the CgPN is from the ‘4X’, ‘7X’ or ‘9X’ numbering range);
- **Phase 2:** Measures to address smishing; and
- **Phase 3:** Extend **Phase 1** to include also incoming calls over international network interfaces with potentially spoofed national CgPN from the ‘4X’, ‘7X’ or ‘9X’ numbering range.

Drawing on the preliminary feedback provided by the local operators forming part of the ad hoc steering committee, the MCA understands that, at this point, it would be more appropriate to focus on some of the measures proposed under **Phase 1**. In particular, the feedback received confirmed that, at this stage, preventative measures targeting incoming calls over international network interfaces with potentially spoofed national CgPN (except where the CgPN is from the ‘4X’, ‘7X’ or ‘9X’ numbering range) would likely represent the best balance between practicability, implementation timeframes, costs, and benefit.

² The term “locally authorised” refers to a situation where an undertaking is notified for a general authorisation with the MCA to provide specific ECN and/or ECS in accordance with its respective general authorisation category (e.g. voice communications services, public electronic communications networks, etc.). Locally authorised undertakings are included in the Register of Authorised Undertakings for providers of ECN and/or ECS, which is publicly available on the MCA’s website.

1.3 Scope

The principal scope for this Consultation Paper is to propose preventative measures, implementable at the technical (network) level, that can mitigate the number of calls, destined towards Maltese numbers, where scammers spoof national numbers to perpetrate a vishing scam. This Consultation Paper is restricted to proposed preventative measures that would fall under the scope of **Phase 1**, as described above.

It therefore does not address potential preventative measures targeting other forms of ECS-based scams, such as those involving SMS with manipulated Sender IDs (smishing), or vishing scams where the CgPN is from the '4X', '7X' or '9X' numbering range. Whilst the MCA recognises that such scams may also lead to end-user harm, it is also of the view that such measures, (which would correspond to those under **Phase 2** and **Phase 3** as described above), merit more extensive study before proceeding to public consultation.

1.4 Definitions and Abbreviations

1.4.1 Definitions

For the purposes of this Consultation Paper, the following definitions shall apply:

Term	Definition
CLI Spoofing	A technique that enables the originating party and/or any network operator handling the call to manipulate the information displayed in the CgPN field with the intention of deceiving the receiving party or the network operators intervening in the handling of the call into thinking that the call originated from another person, entity or location. ³
Maltese Number / National Number	An ITU-T E.164 number ⁴ from the Maltese National Numbering Plan.
Operator of International Network Interfaces	Any undertaking that conveys traffic from networks located outside Malta towards networks located in Malta (including, as applicable, its own network), and vice versa, over its international network interfaces.
Sender ID	An alphanumeric string that can be used as the "From" address for SMS text messages. Whilst legitimate Sender IDs identify the sender by using associated names, brands or phone numbers, scammers sometimes replicate such Sender IDs to pose as the legitimate business/entity.
Sender ID Spoofing	A technique that enables the originating party and/or any network operator handling the message to manipulate the information displayed in the Sender ID field with the intention of deceiving the receiving party or the network operators intervening in the handling of the message into thinking that the message originated from another person, entity or location. ³

³ Adapted from CEPT ECC (2022). *ECC Report 338 - CLI Spoofing*. Accessible at <https://docdb.cept.org/download/4027>

⁴ ITU-T (2010). *The international public telecommunication numbering plan*. Accessible at <https://www.itu.int/rec/T-REC-E.164-201011-I/en>

Term	Definition
Smishing	Fake text messages purporting to be from a legitimate source such as a bank, postal operator or e-commerce site, (generally through the use of Sender ID spoofing), which are used to induce individuals to reveal personal or financial information. ⁵
Vishing	Fake telephone calls purporting to be from a legitimate source such as a bank, postal operator or e-commerce site, (generally through the use of CLI spoofing), which are used to induce individuals to reveal personal or financial information. ⁵

1.4.2 Abbreviations

The following abbreviations are used throughout this Consultation Paper:

Abbreviation	Meaning
AI	Artificial Intelligence
CdPN	Called Party Number(s)
CDR	Call Detail Record
CEPT	European Conference of Postal and Telecommunications Administrations
CFB	Call Forwarding on Busy
CFNRc	Call Forwarding on mobile subscriber Not Reachable
CFNRy	Call Forwarding on No Reply
CgPN	Calling Party Number(s)
CLI	Calling Line Identification
ECC	Electronic Communications Committee
ECN	Electronic Communications Network(s)
ECS	Electronic Communications Service(s)
FTN	Forwarded-To Number
IoT	Internet of Things
ISUP	ISDN (Integrated Services Digital Network) User Part

⁵ Adapted from Interpol, *Social Engineering Scams*. Accessible at <https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams>. Last accessed on 28 September 2023.

Abbreviation	Meaning
ITU-T	International Telecommunication Union's (ITU's) Telecommunication Standardization Sector
M2M	Machine-to-Machine
MCA	Malta Communications Authority
MSRN	Mobile Station Roaming Number
NB-ICS	Number-Based Interpersonal Communications Service(s)
Non-ICS	Non-Interpersonal Communications Service(s)
OTT	Over-the-Top
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
S.L.	Subsidiary Legislation
SMS	Short Message Service
SS7	Signalling System No. 7
STIR	Secure Telephone Identity Revisited
VCS	Voice Communications Services
VLR	Visitor Location Register

1.5 Legal Basis

In accordance with Regulation 80(1) of the Electronic Communications Networks and Services (General) Regulations (S.L. 399.48), the MCA is responsible to establish and manage the national numbering plan for electronic communications services and shall control the granting of rights of use for all national numbering resources.

In this context, and in accordance with Regulation 7(1) and the First Schedule, Part E of S.L. 399.48, the MCA attaches a number of conditions upon granting rights of use for national numbering resources including, but not limited to:

- prohibiting the use of certain numbers as CLI (e.g. numbers from '5X' range);
- requiring that any sub-allocation of national numbers shall be subject to prior authorisation of the MCA, and if authorised, a number of conditions would be determined by the MCA on a case-by-case basis; and
- requiring that sub-allocated national numbers are not used for the provision of voice communications services (VCS).

In view of its mandate on the assignment and rightful use of national numbers, the MCA considers it is of paramount importance, and its duty, to safeguard the public's trust in such numbers and, more generally, in electronic communications networks and services (ECN/S). Scam communications abuse of, and eventually erode such trust, and it is therefore important to the MCA to combat such practices.

Furthermore, Regulation 83(2) of the same S.L. 399.48 mandates that the MCA *"may require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse, and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues."* This regulation empowers the MCA to order such providers to implement measures that lead to the blocking of access to specific numbers or services, depending on the case.

Additionally, it should be noted that in the First Schedule, Part C, point (3) of S.L. 399.48, it is contemplated that the MCA is empowered to attach conditions, tied to the provision of ECS, that constitute *"consumer protection rules specific to the electronic communications sector"*. It is the MCA's view that the imposition of preventative measures to mitigate CLI spoofing and vishing would also contribute to protecting consumers from the harmful effect of scams perpetrated in the domain of electronic communications.

Lastly, it should be noted that criminal investigations of individual cases of ECS-based scams fall outside of the MCA's remit. However, the MCA cooperates with law enforcement authorities whenever it is requested to do so. Furthermore, where the MCA is informed of specific cases of ECS-based scams, it has the right to address any shortcomings arising from non-compliance with relevant MCA Decisions or conditions attached to a general authorisation and/or to the granting of rights of use for numbering resources, amongst others.

2 Proposed Preventative Measures

2.1 High-level Principles

The proposed preventative measures are underpinned by the following high-level principles:

1. **CLI spoofing⁶ is not a practice that is necessary for legitimate calls**, so it is logical to presume that calls using spoofed numbers are intended to deceive the called party and to perpetrate malicious activity. As a minimum, spoofed numbers may include:
 - a. the unauthorised use of an ITU-T E.164 number assigned to a subscriber by another natural or legal person(s) (e.g. a scammer using a number belonging to a bank when originating scam calls);
 - b. the use of an ITU-T E.164 number from vacant numbering ranges; and
 - c. the use of numbers that do not constitute a valid CgPN (e.g. incomplete or incorrect presentation of an ITU-T E.164 number).
2. On the basis of information provided to the MCA, the majority of scam calls with a spoofed Maltese number as CLI are transited into national territory over international network interfaces from abroad. **It is therefore pragmatic to specifically target calls, purporting to be from national numbers, that are received in Malta over such international network interfaces.** Operators of international network interfaces transiting such calls into Malta are thus best placed to take preventative action.
3. Techniques to authenticate call origination information (e.g. STIR/SHAKEN) require significant lead time to be developed and implemented successfully, particularly on a cross-border basis. Moreover, as mentioned in point (2), given that most spoofed calls with a Maltese number as CLI are transited into national territory from abroad, there would be minimal effectiveness of introducing techniques to authenticate call origination information at a local level. Indeed, the involvement of foreign countries would be required for a widespread, and effective, implementation of such techniques on a cross-border basis. **Thus, interventions targeting the authentication of call origination are out of scope of this consultation.**
4. Some solutions, such as over-the-top (OTT) and/or cloud-based communications solutions may also include outbound calling functionalities that permit end-users (typically following prior validations) to set their CLI to any number assigned to them either by other providers ('decoupling'), or the same undertaking providing this ECS solution. Where the said ECS solutions are implemented overseas (hereafter referred to as an 'overseas solution'), calls with a Maltese CgPN destined to other Maltese numbers are likely to appear as incoming calls over operators' international network interfaces. Thus, such calls would fall within scope of the preventative measures.

In this respect, if an undertaking is locally authorised to provide outbound calls and such functionality is implemented through an overseas solution, such calls with a Maltese CgPN would also be legitimate and should, in principle, not be blocked by operators of international network interfaces.

⁶ It should be noted that there could be legitimate reasons for the CLI of an outbound call to be *manipulated* by the caller, (e.g. calls from the mobile phones used by a company's employees presenting the same company's contact number to the called party), but such manipulation would not constitute spoofing if there is no malicious intent.

However, it should be noted that outbound calling functionality with a Maltese CgPN provided by undertakings who are not locally authorised to provide such functionality is not permitted, regardless of whether or not the functionality is implemented through an overseas solution, as this constitutes unauthorised provision of ECS as well as misuse and unauthorised use of Maltese numbering resources.

5. Besides the use-case addressed in point (4) above, the MCA is also sensitive to other legitimate scenarios whereby calls, from a Maltese CgPN, would appear to be incoming over international network interfaces. Thus, **interventions to be implemented should avoid, or minimise, the negative impact on the conveyance of such legitimate calls.** These other legitimate scenarios are addressed in more detail in Section 2.2.
6. Since the **Maltese National Numbering Plan Allocations may evolve over time**, (e.g. updates to designated services for specific numbering ranges, numbering block allocations, etc.), the measures to be implemented should allow room for any necessary updates.

In conclusion, the effectiveness of the measure(s) to be implemented at the international network interfaces needs to be considered against two characteristics, namely the potential for successfully stopping scam calls using spoofed national numbers, and the extent to which the measure can be successful without having a negative impact on the conveyance of legitimate calls.

2.2 Types of Legitimate Calls

This section briefly describes legitimate scenarios whereby calls with a Maltese CgPN would appear to be incoming over the international network interfaces. To assist operators to distinguish between the different legitimate scenarios, three types of calls (Type 'A', Type 'B' and Type 'C') are presented hereunder.

- **Type 'A'**: Calls placed by subscribers assigned national numbers towards national numbers when the calling party is connected to a network outside Malta. In such cases, therefore, the calling party is either:
 - i. an outbound roamer (i.e. CgPN is from the '7X' or '9X' numbering range designated for mobile VCS); or
 - ii. a device used on an extraterritorial basis or in roaming for "limited voice" service in an M2M/IoT context (i.e. CgPN is from the '4X' numbering range designated for non-interpersonal communications services (non-ICS)).
- **Type 'B'**: Calls placed by subscribers assigned national numbers towards inbound roamers in Malta.
- **Type 'C'**: Calls placed by subscribers assigned national numbers towards:
 - i. outbound roamers (assigned Maltese mobile VCS numbers), where the calls would subsequently be late forwarded to a Maltese number (Scenario 1);
 - ii. foreign numbers, where the calls would subsequently be forwarded to a Maltese number (Scenario 2).

Further detailed information on each type of legitimate calls (and respective call flow) is presented in **Annex 1**.

Besides the above, as mentioned in point (4) in Section 2.1, calls placed through an overseas solution offered by a locally authorised ECS provider would also be considered as legitimate calls. In some cases, these overseas solutions provide end-users with the flexibility to associate any of their assigned number(s) as the CLI for outbound calls, regardless of which provider had originally assigned such number(s), albeit this is typically subject to controls or validations as implemented by the respective overseas solution provider. It is therefore not possible to predetermine specific rules, based simply on the analysis of the CgPN and any associated call parameters, to filter out these legitimate calls from other calls where the Maltese number may have been spoofed. In this respect, a bespoke treatment is merited to safeguard the conveyance of legitimate calls placed through such overseas solutions offered by locally authorised ECS providers.

2.3 Preliminary Discussions

During the preliminary discussions with the local operators forming part of the ad hoc steering committee, the MCA presented some 'candidate' measures under **Phase 1**. All measures hereunder would be applicable to incoming calls (towards Maltese numbers) over international network interfaces where the CgPN is a national number.

- **Candidate Measure 1** would mandate the suppression or replacement of the CLI for all incoming calls over international network interfaces with a national CgPN, except in the case of Type 'A' and 'B' calls.
- **Candidate Measure 2(a)** would mandate the blocking of all incoming calls over international network interfaces with a national CgPN, except in the case of Type 'A', 'B' and 'C' calls.
- **Candidate Measure 2(b)** would mandate the blocking of all incoming calls over international network interfaces with a national CgPN, except in the case of Type 'A' and 'B' calls.
- **Candidate Measure 3** would mandate the blocking of incoming calls over international network interfaces where the national CgPN was voluntarily included in a blacklist by its rightful user (e.g. bank, government department, etc.)
- **Candidate Measure 4** would mandate the blocking of incoming calls over international network interfaces where the national CgPN is either from the list of unallocated numbering blocks or from the list of inbound-only sub-blocks. It was noted that this measure could also be extended to incoming calls over national network interfaces.
- Other possible measures, such as voice firewalls, were only discussed superficially.

Candidate Measures 1, 2(a)/2(b) and 3 were proposed as mutually exclusive options, whereas Candidate Measure 4 could be implemented alongside any of the other measures. The MCA also presented the possibility of evolving the measures over time, such as commencing with Candidate Measures 1 or 3 within a short timeframe, and then evolving towards Candidate Measure 2(a) or 2(b).

Further detailed information on Candidate Measures 1 to 4 above, as presented during the preliminary discussions, is included in **Annex 2**. This Annex also presents the insights gained by the MCA during these preliminary discussions.

2.3.1 Feedback Received during Preliminary Discussions

Drawing on the feedback obtained during the preliminary discussions, a comparative table summarising the candidate measures under **Phase 1** is presented in Table 1, together with a high-level analysis of each measure's key benefits and associated risks or limitations.

Key Benefit(s)	Risks or Limitations
Candidate Measure 1. Suppress or replace CLI for all calls with national CgPN; exceptions for Type 'A' & 'B' Calls	
<p>Mitigates the effectiveness of scam calls that rely on spoofed national numbers (except where the CgPN is from the '4X', '7X' or '9X' numbering range).</p> <p>No call is blocked, which eliminates the risk of 'false positives' (i.e. legitimate calls that end up blocked).</p>	<p>Scam calls would still reach the called party.</p> <p>Type 'C' calls would be conveyed with a suppressed/replaced CLI. (Calls where the CgPN is from the '4X', '7X' or '9X' numbering range would not be affected).</p> <p>Calls with suppressed CLI may create difficulties to apply wholesale termination rates.</p> <p>Replacing the CLI would require the use of dedicated numbering (sub-)blocks.</p>
Candidate Measure 2(a). Blocking of all calls with potentially spoofed national CgPN; exceptions for Type 'A', 'B' & 'C' Calls	
<p>Can prevent almost all calls with spoofed national numbers from reaching subscribers assigned Maltese numbers (except where the CgPN is from the '4X', '7X' or '9X' numbering range).</p>	<p>Can result in uncertainty regarding Type 'C' calls where the CgPN is from the '1X', '2X' or '8X' numbering range, as some calls may be blocked due to the absence or limited availability of forwarding information. (Calls where the CgPN is from the '4X', '7X' or '9X' numbering range would not be affected).</p>
Candidate Measure 2(b). Blocking of all calls with potentially spoofed national CgPN exceptions for Type 'A' & 'B' Calls	
<p>Can prevent almost all calls with spoofed national numbers from reaching subscribers assigned Maltese numbers (except where the CgPN is from the '4X', '7X' or '9X' numbering range).</p> <p>End-users with blocked Type 'C' calls can be assisted more easily (when compared with end-user uncertainty for Candidate Measure 2(a)).</p>	<p>Would block all Type 'C' calls where the CgPN is from the '1X', '2X' or '8X' numbering range. (Calls where the CgPN is from the '4X', '7X' or '9X' numbering range would not be affected).</p>
Candidate Measure 3. Blocking of calls where the CgPN is a 'blacklisted' number	
<p>Provides an opportunity to selectively block calls spoofing numbers belonging to high-risk subscribers.</p> <p>Mitigates the effectiveness of scam calls that rely on spoofing known and trusted numbers.</p> <p>Calls where the CgPN is not in the blacklist are not blocked, reducing the risk of 'false positives' (i.e. legitimate calls that end up blocked).</p>	<p>Delays the call set-up process: the larger the blacklist, the longer the delay gets.</p> <p>Requires a robust governance and coordination framework to be successful.</p> <p>Does not protect end-users against spoofing scams that rely on numbers from unallocated numbering blocks, or known and trusted numbers excluded from the blacklist.</p>
Candidate Measure 4. Blocking of calls with CgPN from unallocated blocks or inbound-only sub-blocks	
<p>Blocks calls that are guaranteed to be spoofing or misusing numbers (since CgPN is from unallocated blocks or 'inbound-only' sub-blocks).</p> <p>Does not require extensive governance and coordination beyond the initial implementation phase and potential subsequent updates, which are not expected to be frequent.</p> <p>Can be implemented for all calls, not just those received over international network interfaces.</p>	<p>Delays the call set-up process: the larger the list of numbering blocks or sub-blocks to be checked, the longer the delay gets.</p> <p>Does not protect end-users against spoofing of numbers from allocated numbering blocks, particularly known and trusted numbers. Thus, mainly considered to be implemented alongside other measures rather than on its own.</p>

Table 1 – Summary of Candidate Measures and Feedback Received during Preliminary Discussions

2.3.2 Conclusions from Preliminary Discussions

The feedback received during the preliminary discussions provided the MCA with reliable insights on the potential effectiveness, practicability, key benefits and risks or limitations of each measure proposed under **Phase 1**, as summarised above. On the basis of this feedback, and insights gleaned from desk research carried out, the MCA considers that Candidate Measures 2(b) and 4 represent an ideal starting point to effectively target calls with spoofed national numbers, whilst limiting the impact on the conveyance of legitimate calls.

2.4 The Framework of Interventions

The MCA is hereunder proposing a framework of interventions to mitigate CLI spoofing and vishing scams. When factoring in the principle of technology neutrality, the MCA considers it imperative that any preventative measures adopted shall apply irrespective of the technology used for call conveyance over international network interfaces (e.g. ISUP (part of SS7), SIP, etc.). Furthermore, in the Proposed Decisions, indicative implementation timeframes are being provided in terms of elapsed time (in weeks) from the date of publication of the respective Decision Notice (hereafter “publication date”).

2.4.1 Incoming Calls with CgPN from ‘1X’, ‘2X’ or ‘8X’ Numbering Range

With a view to target scams which spoof national numbers in the ‘1X’ (short codes), ‘2X’ (fixed VCS) and ‘8X’ (freephone) numbering ranges, the MCA considers that operators of international network interfaces should block all incoming calls over such interfaces where the CgPN pertains to the ‘1X’, ‘2X’ or ‘8X’ numbering range, except – to safeguard Type ‘B’ calls (i.e. calls to inbound roamers in Malta) – where the called party number (CdPN) is a Maltese Mobile Station Roaming Number (MSRN).

It should be noted that calls with CgPN from the mobile VCS numbering ranges (‘7X’ and ‘9X’) and non-ICS numbering range (‘4X’) are also being excluded from this intervention, given that calls may originate from subscribers or devices assigned these numbers whilst connected to a foreign network (e.g. whilst roaming abroad). This exclusion would therefore safeguard the conveyance of all Type ‘A’ calls.

In keeping with the principle of (only) allowing legitimate calls to be conveyed, providers may also implement rule-based filters to block calls where the CgPN is from the unallocated sub-ranges from the ‘4X’, ‘7X’ or ‘9X’ numbering range. Drawing on the preliminary feedback obtained, the MCA recognises that such increased granularity may have a negative impact on call set-up time for some operators, due to the increased number of checking taking place on a real-time basis. Thus, such additional granularity is not being mandated in *Proposed Decision 1*. However, where this is implemented, it would invariably improve this intervention’s effectiveness to mitigate scam calls.

Lastly, the MCA wishes to clarify that this intervention is primarily based on Measure 2(b), as proposed during the preliminary discussions, which garnered significant support from all local operators during the preliminary discussions. This variant of Candidate Measure 2 did not contemplate any rule-based filters to specifically cater for Type ‘C’ calls, and it is thus envisaged that all such calls originated with a CgPN from the ‘1X’, ‘2X’ or ‘8X’ numbering range would be blocked. This limitation is further discussed in sub-section 2.4.2 below.

The MCA is thus proposing the following:

Proposed Decision 1

Operators of international network interfaces are to block all incoming calls over such interfaces with a Maltese CgPN from the '1X', '2X' or '8X' numbering range, except for calls where the CdPN corresponds to a Maltese MSRN served either by the same operator, or any other locally authorised provider that offers inbound roaming services.

Decision 1 will apply with effect from [sixteen (16) weeks from the publication date].

With a view to oversee the effective implementation of *Proposed Decision 1*, the MCA is establishing the following framework of obligations:

Proposed Decision 2

The following obligations shall apply:

- a. All locally authorised providers of inbound roaming services are to provide the MCA with the list of mobile VCS numbering (sub-)blocks being used for the purposes of associating MSRNs to calls towards inbound roamers served on their network (hereafter "MSRN (sub-)blocks").
 - Provided that the MSRN (sub-)blocks should be communicated to the MCA by no later than [four (4) weeks from the publication date] for providers already authorised to provide inbound roaming services at the time of publication of this Decision Notice; and
 - Provided that, for undertakings who intend to start providing inbound roaming services after the publication of this Decision Notice, the MSRN (sub-)blocks are to be communicated to the MCA at least sixty (60) calendar days in advance of the planned date of commencement of inbound roaming services provision.
- b. Without prejudice to point (c) below, providers of inbound roaming services are to associate MSRNs to calls towards inbound roamers solely from the MSRN (sub-)blocks communicated under point (a) above.
- c. Where changes to the communicated MSRN (sub-)blocks are necessary and justified, the respective provider who wishes to implement these changes is to allow sufficient time for these changes to be communicated to, and subsequently implemented by, all locally authorised operators of international network interfaces. With a view to facilitate this process, the MCA is to be informed at least thirty (30) calendar days in advance of this provider's planned date for implementing such changes.
 - Provided that the MCA may require the respective provider to extend the planned date for implementation under certain justified circumstances, for instance, to take into account industry practices such as network data freezes which are carried out by the operators.
- d. Within five (5) working days of receiving complete information in terms of points (a) and/or (c) above, the MCA will circulate this information solely amongst locally authorised operators of international network interfaces.

2.4.2 Impact on Type 'C' Calls

As introduced in Section 2.2 above, Type 'C' calls comprise either:

- a. calls placed by subscribers assigned Maltese numbers towards outbound roamers (also assigned Maltese mobile VCS numbers), where the calls would subsequently be late forwarded⁷ to another Maltese number; or
- b. calls placed by subscribers assigned Maltese numbers towards foreign numbers, where the calls would subsequently be forwarded (conditionally or unconditionally) towards another Maltese number.

In the case of (a) above, the Forwarded-to Number (FTN) may, for example, be another Maltese number assigned to the called subscriber, or perhaps the number associated with the voicemail service offered by the respective service provider. As regards case (b), consider the example of an office in a foreign country belonging to a person who travels frequently between Malta and this foreign country for work. Such forwarding setup would assist this person to minimise the number of missed calls during times when the office abroad is unmanned as calls to this office number would be forwarded towards the Maltese number set as the FTN.

In both cases (a) and (b) above, the incoming calls (towards the Maltese FTN) would appear over the international network interfaces whilst bearing a Maltese CgPN (as further explained in **Annex 1**). In this regard, a specific measure that could assist operators to distinguish Type 'C' calls from other incoming calls would be to base the rule-based filters on the provided forwarding-related information⁸ and the presence of a Maltese FTN.

Nevertheless, during the preliminary discussions, it emerged that such forwarding-related information is rarely, if ever, sent along for calls forwarded over international network interfaces. Thus, whilst such real-time rule-based filters could assist to identify *some* Type 'C' calls, it is not possible to identify all Type 'C' calls given the restricted information being received by operators of international network interfaces.

Given this context, the MCA considers that it would not be practicable to mandate the implementation of rule-based filters intended to specifically identify Type 'C' calls based on analysing forwarding-related information. Indeed, mandating such a practice would still result in some calls being blocked, due to the absence of the forwarding-related information, whilst a subset of Type 'C' calls would be allowed through. Such a situation would result in uncertainty around whether calls would be successfully conveyed.

It could be argued that end-users would be better off knowing that a *specific* subset of forwarded calls would be blocked outright, rather than being told that the calls may or may not be blocked. Such certainty would indeed allow end-users to make alternative arrangements as applicable. The MCA understands that providing such certainty to end-users could also make it easier for providers to troubleshoot subscribers' issues in this regard.

⁷ Late call forwarding is being used to refer to call forwarding which takes place after the call has reached the visited network of the forwarding subscriber. Examples of late call forwarding include call forwarding on busy (CFB), call forwarding on no reply (CFNRy), and call forwarding on mobile subscriber not reachable (CFNRc) when forwarding takes place in the visited network.

⁸ 'Forwarding-related information' refers to the information passed on between operators on any forwarding activity for that call.

To be clear, if *Proposed Decision 1* is implemented as described above, where a subscriber places a Type 'C' call with a CgPN from the '1X', '2X' or '8X' numbering range, then the call would end up being blocked.⁹ This would indeed correspond to a scenario where a legitimate call would have been blocked as a result of the proposed preventative measure.

The limited forwarding-related information made available to local operators also means that, regrettably, the MCA cannot forecast the extent of the potential impact on Type 'C' calls where the CgPN are from numbering ranges subject to the blocking intervention in *Proposed Decision 1* (i.e. '1X', '2X' and '8X'). Indeed, the data received by local operators when conveying such calls cannot reliably shed light on the total quantity of calls with a Maltese FTN, given that not all Type 'C' calls are accompanied by the forwarding-related information which is necessary to identify them as such. Furthermore, following enquiries with locally authorised VCS providers, it transpires that information in Call Detail Records (CDRs) for calls made by (Maltese) outbound roamers is also of limited value, as the data in the CDRs do not allow a distinction to be made between calls originated by the outbound roamer, or calls that were received by the outbound roamer and subsequently forwarded to a Maltese FTN. In conclusion, the available data on the extent of such calls are more likely to mislead, rather than assist the MCA's decision-making.

Notwithstanding, with a view to 'cushion' the potential impact of blocking some Type 'C' calls, the MCA considers that some transparency measures need to accompany the introduction of any new blocking measure to be implemented. In this regard, the MCA will endeavour to communicate the impact on some Type 'C' calls through its various channels interfacing with the general public.

Besides the above, the MCA also considers that local VCS providers are in a better position to reach out to the general public, through their subscription base, and is therefore proposing the implementation of mandatory transparency measures in *Proposed Decision 3*, as follows (next page).

⁹ It is assumed that, under normal circumstances, a subscriber would not set a number corresponding to an MSRN as his/her FTN. In this regard, the implication of *Proposed Decision 1* is that a Type 'C' call would be blocked where the CgPN is from the '1X', '2X' or '8X' numbering range. However, there should be no blocking of Type 'C' calls where the CgPN is from the '4X', '7X' or '9X' numbering range.

Proposed Decision 3

By no later than [six (6) weeks from the publication date], locally authorised VCS providers are to ensure that all their subscribers assigned numbers from the '1X', '2X', '7X', '8X' or '9X' numbering range are made aware of the potential impact of Decision 1 on the conveyance of Type 'C' calls.

- a. This shall be done through relevant updates to the Terms and Conditions which should, as a minimum, provide:
 - i. an explanation to their subscribers that some forwarded calls may be blocked, either by their provider or other locally authorised providers, in accordance with this Decision Notice;
 - ii. the date from when such blocking intervention will be in force; and
 - iii. provide information on a suitable channel which the subscriber may avail of to obtain additional information on this blocking intervention.
- b. Providers are to notify their subscribers of the updates to the Terms and Conditions as per (a) above in accordance with the processes as established in regulation 92 of S.L. 399.48 and the MCA's Decision Notice '*Contracts, Transparency and Termination of Services*' (MCA-D/yc/23-4851).
- c. Providers are to ensure that the information contained in (a)(i) to (a)(iii) above is also included, where relevant, in the Terms and Conditions for any new services and/or tariff plans which providers may launch from time to time.
- d. Providers are to publish on their website, information on:
 - i. the potential impact of Decision 1 on the conveyance of Type 'C' calls; and
 - ii. any action(s) that may be taken to mitigate such impact.
- e. The information in (d) above should be published by no later than [six (6) weeks from the publication date] and retained online for at least six (6) months from the [effective date of Decision 1].

In addition to the information in point (d) of *Proposed Decision 3*, providers are encouraged to leverage additional channels to facilitate access to information to subscribers who may not be familiar with navigating online content. In this regard, relevant information on the foreseen impact may also be included in any bills or other official communication sent to subscribers from time to time, and/or in any printed literature supplied to subscribers visiting the providers' outlets. Customer care agents are also encouraged to relay this information when interacting with subscribers to assist them setting up such forwarding services, regardless of whether this interaction is on face-to-face basis or via other approaches.

Lastly, for new entrants in the provision of locally authorised VCS, respective timeframes to comply with *Proposed Decision 3* would be communicated by the MCA, taking into account the commencement date of operations for such new entrant.

2.4.3 Incoming Calls with CgPN from '3X', '5X' or '6X' Numbering Range

Where a call over the international network interfaces bears a CgPN pertaining to the '3X', '5X' or '6X' numbering range, the MCA considers that it would be appropriate to block the call since:

- Numbers in the '5X' numbering range are assigned to premium rate service providers and should not be presented as CLI for outbound calls in accordance with the conditions outlined in the MCA's Decision Notice "*A Framework for Premium Rate Services in the '5' Numbering Range*" (MCA/10/58/D). In this Framework, it is noted in Decision 5.1 that operators are to prevent the use of a premium rate number as CLI, because such numbers may be used inadvertently by the called party when returning a call. It is worth recalling that leaving missed calls with a premium number as CLI is indeed the 'modus operandi' of scammers behind so-called 'Wangiri' scam calls.
- There are currently no allocations to locally authorised providers in the '3X' numbering range, whereas the '6X' numbering range is vacant at present. Consequently, it is justified to block calls with a CgPN from these numbering ranges, as the use of a '3X' or '6X' number would correspond to a case of CLI spoofing or other misuse of national numbers.

The MCA is therefore proposing that:

Proposed Decision 4

Operators of international network interfaces are to block all incoming calls over such interfaces with a Maltese CgPN from the '3X', '5X' or '6X' numbering range, regardless of the CdPN.

Decision 3 will apply with effect from [sixteen (16) weeks from the publication date].

2.4.4 Intervention related to Overseas Solutions offered by ECS providers

As mentioned in both Sections 2.1 and 2.2 above, calls with a Maltese CgPN towards national numbers placed through overseas solutions may also appear to operators as incoming calls over their international network interfaces. All such calls would therefore be subject to the rule-based filters envisaged in the proposed preventative measures, and it should therefore be clarified that these calls would be legitimate solely where the calls are originated via the overseas solutions offered by locally authorised ECS providers.

The above is based on the premise that advancements in technology provide end-users with some flexibility in terms of associating assigned number(s) with call origination services, for instance:

- originating calls via an overseas solution provided by the same service provider offering call termination services for the said number(s); or
- decoupling call origination from call termination through, for example, cloud-based communications or OTT overseas solutions provided by (third party) locally authorised ECS providers.

Thus, whilst the service provider for call termination services may rightfully only be the serving provider for that number at that point in time, there could, on the other hand, be more than one service provider offering (legitimate) call origination services associated with the same number assigned to a subscriber.

Besides the above, the MCA is aware that the provision of services through such overseas solutions may also be bundled with integrated systems offerings that facilitate aspects, such as customer relationship management, that extend beyond the connectivity services typically offered by VCS providers. Such integrated systems may be mission-critical to certain business users, and any impact on the connectivity aspects of such integrated systems should be carefully considered. Indeed, absent any specific intervention to sustain the authorised provision of such overseas solutions, the implementation of *Proposed Decision 1* would imply that calls originated in this manner would be blocked, unless either:

- a. the CgPN is from the '1X', '2X' or '8X' numbering range and the CdPN is a Maltese MSRN, or
- b. the CgPN is from the '4X', '7X' or '9X' numbering range.

This limitation in the *connectivity* aspect would reduce the practical usefulness of these overseas solutions and may have a negative impact on the performance of businesses whose operations depend on such integrated systems. Unless rectification measures are implemented, the blocking intervention would result in an impact regardless of whether the solutions being relied on are being offered by locally authorised ECS providers, or otherwise. In this respect, whilst the MCA recognises that the proposed blocking interventions would have a positive effect through diminished scam calls, the potential for a negative impact, particularly on the business community, should be anticipated and addressed *a priori*.

Such an impact may be prevented if calls originating from such overseas solutions are not 'mixed' with other incoming calls received over operators' international network interfaces, that is, such calls would be transited towards the called party through a *distinct* path that 'bypasses' the rule-based filters implemented on the international network interfaces.

To achieve such separation for calls originated via these overseas solutions, it would be necessary for the respective ECS provider to pre-establish a distinct, dedicated interface between its overseas solution and at least one locally authorised provider of *Public Electronic Communications Networks* and *Voice Communications Services* with a Point of Interconnection in Malta. This dedicated interface, which may, for example, take the form of a dedicated SIP trunk between the two parties, would be the sole path used for all calls, originated via the overseas solution, where both the CgPN and the CdPN are numbers from the Maltese National Numbering Plan. With this setup in place, it would be ensured that all such calls would be 'brought in' to Malta via the dedicated interface(s), rather than over international network interfaces.

It should be clarified that bypassing the rule-based filters via the dedicated interface would only be acceptable, and therefore permitted, subject to the following:

- a. The undertaking offering the overseas solution would have to be notified with the MCA for a general authorisation, under the applicable category(ies), to provide number-based interpersonal communications services (NB-ICS) in Malta. Failure to satisfy this requirement would imply that this undertaking would be unauthorised to provide such a NB-ICS in Malta. Accordingly, it would be justified to implement measures that block calls originated through the overseas solution of this unauthorised undertaking.

- b. The undertaking offering the overseas solution should ensure that dedicated interfaces are only utilised for conveying legitimate calls towards Maltese numbers originated by validated end-users. Thus, if or where such undertaking becomes aware of calls originated through its overseas solution where there is misuse, unauthorised or fraudulent use of numbers, it shall be held accountable to address the matter with the respective end-users. Where the matter remains unresolved, the MCA would consider this a breach of such undertaking's duty of care obligations and may order the respective undertaking to terminate any relevant relationship with third parties where there is evidence of misuse, unauthorised or fraudulent use of numbers or services.
- c. Where an undertaking persistently or repeatedly fails to comply with the MCA's directions, the MCA reserves the right to order all locally authorised providers to cease service provision via any dedicated interfaces established with the said undertaking.

Thus, for undertakings to offer NB-ICS via such overseas solutions to end-users in Malta, particularly the provision of outbound calling functionality where the end-user may set a Maltese number as CLI, the MCA is proposing two interrelated Decisions, whereby *Proposed Decision 5* is intended to govern aspects related to the general authorisation for such undertakings, and the rightful use for numbering resources in such service provision, whereas *Proposed Decision 6* mandates the setting up and the expected use of the aforementioned dedicated interface(s).

The MCA therefore proposes:

Proposed Decision 5

The association of a Maltese number as CLI with an outbound call placed via an undertaking's overseas solution is not permitted, except where the undertaking fulfils both criteria hereunder, namely:

- a. the undertaking is notified as a locally authorised provider of NB-ICS with the MCA, that is, it would be authorised, depending on the services offered, as either:
 - i. a provider of *Voice Communications Services*, or
 - ii. a provider of *Other Electronic Communications Services* for the sub-category *Number-Based Interpersonal Non-Voice Communications Services*; and
- b. the undertaking offering services through overseas solutions must employ subscriber validation processes and is able to ensure that such solutions are only utilised for conveying calls by validated end-users.

The above-mentioned exception shall be without prejudice to any other condition that may be attached to the general authorisation and/or to the granting of rights of use for numbering resources.

The MCA further proposes:

Proposed Decision 6

Further to satisfying the obligation emanating from Decision 5, where an undertaking's overseas solution permits outbound calling with a Maltese CgPN from the '1X', '2X' and/or '8X' numbering range, that undertaking is required to establish a dedicated interface with at least one (1) locally authorised provider of *Public Electronic Communications Networks* and *Voice Communications Services* with a Point of Interconnection in Malta;

- Provided that such dedicated interface may also be set up on an 'internal basis' if the overseas solution is provided by an undertaking that is a locally authorised provider of *Public Electronic Communications Networks* and *Voice Communications Services* with a Point of Interconnection in Malta.

By no later than [ten (10) weeks from the publication date], all calls originated via an undertaking's overseas solution, where both the CgPN and the CdPN correspond to a number in the Maltese National Numbering Plan, shall reach the Maltese territory solely via any established dedicated interface(s).

With a view to allow time for any undertakings offering such overseas solutions to regularise their situation and comply with Decision 5 and this Decision 6, the MCA requests all locally authorised ECS providers to refrain from implementing any *ad hoc* (interim) interventions which seek to identify and block calls originated in this manner prior to the coming into force of Decision 1.

Furthermore, prior to establishing any dedicated interface with an undertaking offering outbound calls with a Maltese CgPN through overseas solutions, locally authorised providers of *Public Electronic Communications Networks* and *Voice Communications Services* with a Point of Interconnection in Malta are to confirm with the MCA that the said undertaking holds a valid local general authorisation.

As mentioned above, the provision of services through these overseas solutions is at times included in integrated systems offerings that are critical to certain business operations. In this respect, the MCA notes that, when the blocking interventions come into force (i.e. sixteen (16) weeks from the publication date), all calls originated via the overseas solutions of undertakings that do not satisfy *Proposed Decisions 5* and *6* would become subject to blocking in accordance with *Proposed Decisions 1* and *4*.

With a view to mitigate the foreseeable impact on end-users of such overseas solutions, and any potential economic impact, the MCA considers that an intervention is warranted to improve transparency. Besides forewarning end-users of the potential impact, such transparency measures could also act as a trigger for end-users to either find alternative, authorised arrangements, or to solicit their current providers to regularise their position in line with *Proposed Decisions 5* and *6* above.

Given that the principal impact is expected to be felt by business end-users assigned Maltese numbers by locally authorised VCS providers, the MCA considers that the latter's support would be crucial to raise awareness on the foreseeable impacts of the proposed blocking interventions. Furthermore, the MCA considers that locally authorised VCS providers may also be net beneficiaries from this measure, since they may:

- be in a position to offer authorised solutions as an alternative to any overseas solutions offered by unauthorised third parties who would be affected; and
- establish commercial partnerships with undertakings authorised to provide ECS via such overseas solutions who are in the process of setting up the mandatory dedicated interface to regularise their offering.

In this regard, the MCA considers that the obligations on locally authorised VCS providers, as foreseen in *Proposed Decision 7*, are not only in the interest of the same locally authorised VCS providers, but are also justified on grounds of national interest and to safeguard the end-users subscribed to services offered via such overseas solutions.

Proposed Decision 7

By no later than [six (6) weeks from the publication date], locally authorised VCS providers are to ensure that all their subscribers assigned numbers from the '1X', '2X' or '8X' numbering range are made aware of the potential impact of Decisions 1, 5 and 6 on the conveyance of calls originated via overseas solutions of unauthorised undertakings.

- a. This shall be done through relevant updates to the Terms and Conditions which should, as a minimum, provide:
 - i. an explanation to their subscribers that calls originated via the overseas solutions of unauthorised undertakings may be blocked, either by their provider or other locally authorised providers, in accordance with this Decision Notice;
 - ii. the date from when such blocking intervention will be in force; and
 - iii. provide information on a suitable channel which the subscriber may avail of to obtain additional information on this blocking intervention.
- b. Providers are to notify their subscribers of the updates to the Terms and Conditions as per (a) above in accordance with the processes as established in regulation 92 of S.L. 399.48 and the MCA's Decision Notice '*Contracts, Transparency and Termination of Services*' (MCA-D/yc/23-4851).
- c. Providers are to ensure that the information contained in (a)(i) to (a)(iii) above is also included, where relevant, in the Terms and Conditions for any new services and/or tariff plans which the providers may launch from time to time.
- d. Providers are to publish on their website, information on:
 - i. the potential impact of Decisions 1, 5 and 6 on the conveyance of calls originated via overseas solutions of unauthorised undertakings; and
 - ii. any action(s) that may be taken to mitigate such impact.
- e. The information in (d) above should be published by no later than [six (6) weeks from the publication date] and retained for at least six (6) months from the [effective date of Decision 1].

Given that the potential impact of *Proposed Decisions 1, 5 and 6* may also extend to critical business operations of end-users availing of these overseas solutions, providers are encouraged to leverage additional channels to facilitate access to information on this potential impact over and above those prescribed in point (d) above.

In this regard, relevant information on the foreseeable impact may also be included in any bills or other official communication sent to subscribers from time to time, and/or in any printed literature supplied to subscribers visiting the providers' outlets. Providers may also consider reaching out directly to subscribers on business tariffs. Depending on available business intelligence, such outreach could be targeted to a specific sub-set of subscribers that are more likely to be using such overseas solutions.

Further to the above, for new entrants in the provision of locally authorised VCS, respective timeframes to comply with *Proposed Decision 7* would be communicated by the MCA, taking into account the commencement date of operations for such new entrant.

Lastly, the MCA considers that, for an interim period prior to the coming into force of *Proposed Decision 1*, it would be beneficial for end-users of such overseas solutions to be presented with a pre-recorded voice announcement whenever they place outbound calls which would have been blocked had the blocking intervention been active. Such announcements would need to be played to the caller by the operator of the international network interface prior to establishing the call with the called party.

The MCA is therefore proposing that:

Proposed Decision 8

As from [the start of the eleventh (11th) week from publication date], operators of international network interfaces are to introduce a facility for a pre-recorded voice announcement to be played to the caller for all calls which would have been blocked had the blocking intervention in Decision 1 been active. Such announcements would be played prior to establishing the call with the called party. This facility shall remain in place until the coming into force of Decision 1.

As a minimum, the pre-recorded voice announcement should be in both English and Maltese, and include:

- an explanation that the call would be blocked as from [sixteen (16) weeks from the publication date]; and
- an invitation to seek out additional information from the calling party's provider if needed.

Due time should be allowed by operators to ensure that the pre-recorded voice announcement is not activated prior to the MCA's approval. In this regard, operators are to submit a script of the planned voice announcement to the MCA at least five (5) working days in advance of its recording.

The MCA acknowledges that the above announcement would not only be played for calls originated through overseas solutions provided by undertakings that have not yet fulfilled the conditions in *Proposed Decisions 5* and *6*, but also in the case of Type 'C' calls with a CgPN from the '1X', '2X' or '8X' numbering range.

Besides the steps that need to be taken by locally authorised VCS providers and providers of international network interfaces in accordance with *Proposed Decisions 7* and *8* above, the MCA will also endeavour to raise awareness on this topic in due course to ensure further transparency on the potential impact.

3 Performance Monitoring

The implementation of the blocking interventions at the network level would only constitute a first step in the fight against these vishing scams. Accordingly, following such implementation, it would be crucial to monitor the effectiveness of these interventions against the stated goal of mitigating scam calls whilst safeguarding legitimate calls.

In this regard, the MCA considers that the technical solutions to be implemented by operators of international network interfaces should also permit sufficient performance logging to draw insights on the effectiveness of the measures. Thus, the technical solutions should provide the said operators with the ability to extract data or logs with sufficient detail to report statistical information to the MCA, as a minimum, on:

- a. The total number of incoming calls blocked by the operator; and
- b. The distribution, per CgPN prefix, of the number of incoming calls blocked by the operator.

In this regard, the MCA is proposing the following:

Proposed Decision 9

Operators of international network interfaces subject to implement the blocking interventions mandated in Decisions 1 and 4 are to be able to extract data or logs from the implemented solution comprising sufficient detail to provide the MCA with statistical information, as a minimum, on:

- a. the total number of incoming calls blocked by the operator; and
- b. the distribution, per CgPN prefix, of the number of incoming calls blocked by the operator by virtue of Decisions 1 and 4.

Such statistical information may be requested by the MCA from time to time.

Further insights on the effectiveness of the intervention may also be gleaned from the number of subscribers complaining about scam calls, or related impacts. Thus, the MCA also considers it appropriate for locally authorised VCS providers to keep records of the nature and quantity of such complaints. Correspondingly, the MCA may also leverage insights on the effectiveness of the intervention from related complaints made directly with the MCA itself.

Such insights may also facilitate the MCA's planning and priorities for any future interventions, for instance, by informing the MCA on what measures may require updating, or whether to proceed to a next phase of interventions.

Lastly, with regard to *Proposed Decisions 5 and 6*, the MCA recognises that the interventions to be implemented are novel and may require specific monitoring with a view to prevent potential abuse. Thus, the MCA reserves the right to revisit these interventions if it becomes aware that the dedicated interfaces are either being abused to convey scam calls by circumventing the rule-based filters at operators' international network interfaces, or if the dedicated interfaces are used to *transit* calls originated from unauthorised undertakings, in addition to conveying calls originated from an authorised overseas solution.

4 Implementation Timeframes

A summary of the implementation timeframes included in the above *Proposed Decisions* is presented in Table 2 below.

Proposed Decision	Elapsed weeks
Proposed Decision 1	16 weeks from publication date
Proposed Decision 2	4 weeks from publication date
Proposed Decision 3	6 weeks from publication date
Proposed Decision 4	16 weeks from publication date
Proposed Decision 5 and 6	10 weeks from publication date
Proposed Decision 7	6 weeks from publication date
Proposed Decision 8	Starting from the 11 th week from publication date, until the blocking intervention is introduced.
Proposed Decision 9	16 weeks from publication date

Table 2 - Implementation timeframes included in Proposed Decisions

The above timeframes are reflected in the Graphical Timeline below (Figure 1). It should be noted that *Proposed Decision 5* does not specifically refer to a timeframe, although the corresponding obligation is linked with that in *Proposed Decision 6*. Furthermore, whilst *Proposed Decision 9* is not associated with a specific timeframe, it can only be enforceable once the blocking interventions go live (i.e. 16 weeks from publication date, as per above).

Indicative Implementation Timeframes		Elapsed weeks from Publication Date of Decision Notice																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Milestone 1	MCA to be informed on MSRN (sub-)blocks as per <i>Proposed Decision 2</i>	█																
Milestone 2	Update to T&Cs and other transparency measures as per <i>Proposed Decisions 3 and 7</i>	█																
Milestone 3	Undertakings with overseas solutions to regularise their position as per <i>Proposed Decisions 5 and 6</i>	█																
Milestone 4	Pre-recorded announcement as per <i>Proposed Decision 8</i>												█					
Milestone 5	Blocking interventions as per <i>Proposed Decisions 1 and 4</i>																	◆

Figure 1 – Proposed Graphical Timeline for Implementation

5 Submission of Feedback

In accordance with the requirements of Article 4A of the Malta Communications Authority Act (Cap. 418 of the Laws of Malta), the MCA invites written submissions from interested stakeholders with feedback on this Consultation Paper and the Proposed Decisions aimed at mitigating CLI spoofing and vishing scams.

The MCA appreciates that respondents may provide confidential information in their feedback to this Consultation Paper. This information is to be included in a separate annex and should be clearly marked as confidential. Respondents are also requested to state the reasons why the information should be treated as confidential. The MCA will take the necessary steps to protect the confidentiality of such material as soon as it is received at the MCA offices in accordance with the MCA's confidentiality guidelines and procedures¹⁰. Respondents are however encouraged to avoid confidential markings wherever possible.

The MCA will, after taking into consideration the responses received to this Consultation Paper, publish a Decision Notice on the preventative measure(s) to be implemented.

For the sake of openness and transparency, the MCA will publish a list of all respondents to this Consultation Paper in the aforementioned Decision Notice.

All responses should be sent to the MCA, by post or e-mail, by not later than 12:00 CET on Tuesday, 31 October 2023, and addressed to:

The Chief of Operations
Malta Communications Authority
Valletta Waterfront, Pinto Wharf
Floriana FRN1913
Malta

Tel: +356 2133 6840

E-mail: coo@mca.org.mt

Extensions to the consultation deadline will only be permitted in **exceptional circumstances** and where the MCA deems fit. The MCA reserves the right to grant or refuse any such request at its discretion.

¹⁰ https://www.mca.org.mt/sites/default/files/articles/confidentialityguidelinesFINAL_0.pdf

Annex 1: Legitimate Call Types

The following figures present simplified call flows for each type of legitimate calls. It should be noted that some additional steps may be involved, and that the figures presume that the CgPN of the originating caller is received by the operator of the international network interfaces.

Type 'A' calls: Calls placed by subscribers assigned national numbers towards national numbers when the calling party is connected to a network outside Malta

In Type 'A' calls, the flow for the call is relatively straightforward. The prerequisite for these calls is that a subscriber assigned a Maltese number, from either the mobile VCS ('7X' or '9X') or non-ICS ('4X') numbering ranges, connects with a network outside of Malta. Such connection is typically established when the subscriber roams internationally, but it can also involve devices connected with their home network abroad if the '4X' number was assigned extraterritorially.

Regardless of how such connection is established, the first step in the call flow for Type 'A' calls is for the subscriber assigned these numbers to initiate a call towards a Maltese number whilst being connected to the foreign network. In such case, the CgPN would be a mobile VCS number from the '7X' or '9X' numbering range, or a number from the '4X' numbering range. This is captured as Step 1 in Figure 2 below, which presents a simplified representation of the Type 'A' call flow.

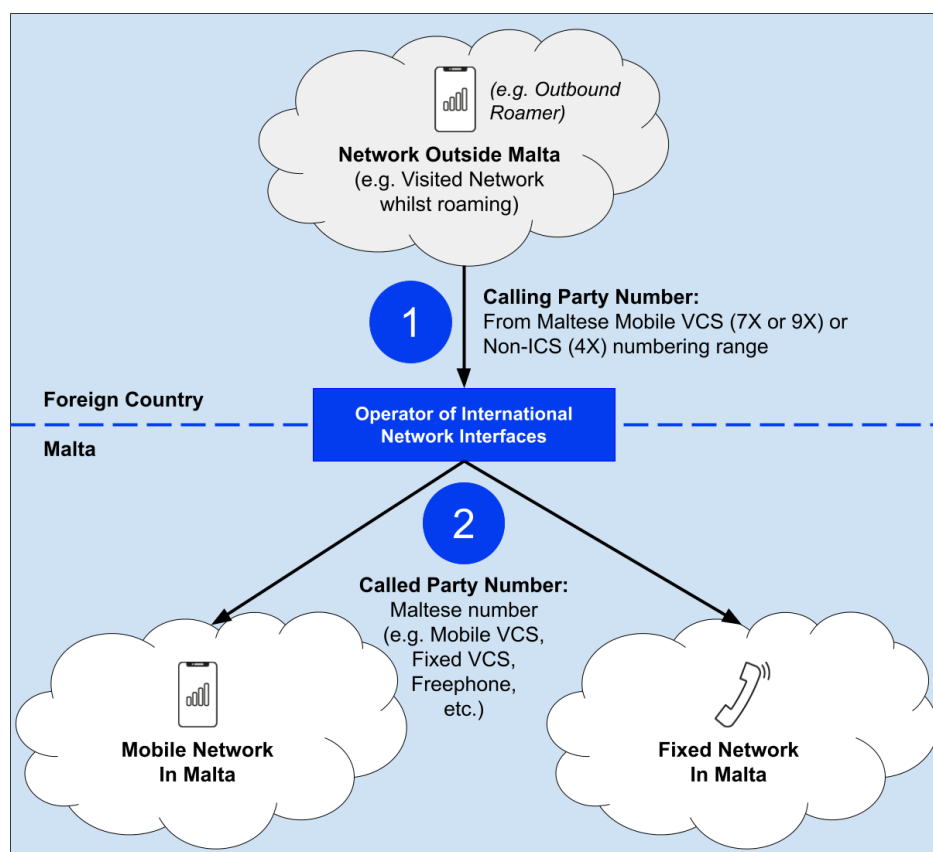


Figure 2 - Simplified flow for Type 'A' calls

From the point of origination onwards, the call is routed towards Malta (given the Maltese CdPN) and various 'hops' may be involved up until the call reaches an operator of international network interfaces. This operator then determines further routing depending on the CdPN, as shown in Step 2.

The operator of international network interfaces that is first to receive the incoming call in Malta may also be providing the subscription network for the CdPN, but this is not always the case, as international conveyance of calls depends on various factors, such as the commercial agreements established between providers. Thus, before the call reaches the subscription network to be subsequently terminated to the called party, further transit may occur in Malta between local providers.

Type 'B' Calls: Calls placed by subscribers assigned national numbers towards inbound roamers in Malta

In Type 'B' calls, the CgPN would be a Maltese number assigned to a subscriber in Malta, whilst the CdPN would be a foreign mobile number belonging to an end-user currently roaming in Malta (i.e. an inbound roamer). As an example, consider the case of a hotel receptionist calling from the hotel's Maltese fixed VCS number towards the foreign mobile number of a guest residing at the same hotel.

Steps 1 and 2 in Figure 3 show the call being initiated by the subscriber assigned a Maltese number (Step 1), whereby (based on the foreign number dialled) the call is first routed, and conveyed over international network interfaces, towards the foreign subscriber's home network abroad (Step 2). At this point, since this foreign subscriber is inbound roaming in Malta, the respective home network would exchange signalling with the visited network in Malta, as per Step 3, to obtain the Maltese MSRN to be associated with the call towards the inbound roamer. Once the Maltese MSRN is obtained by the home network, the call is routed towards Malta and various 'hops' may be involved up until the point that the call reaches an operator of international network interfaces. This operator then determines further routing on the Maltese territory to terminate the call to the intended inbound roamer (Step 4).

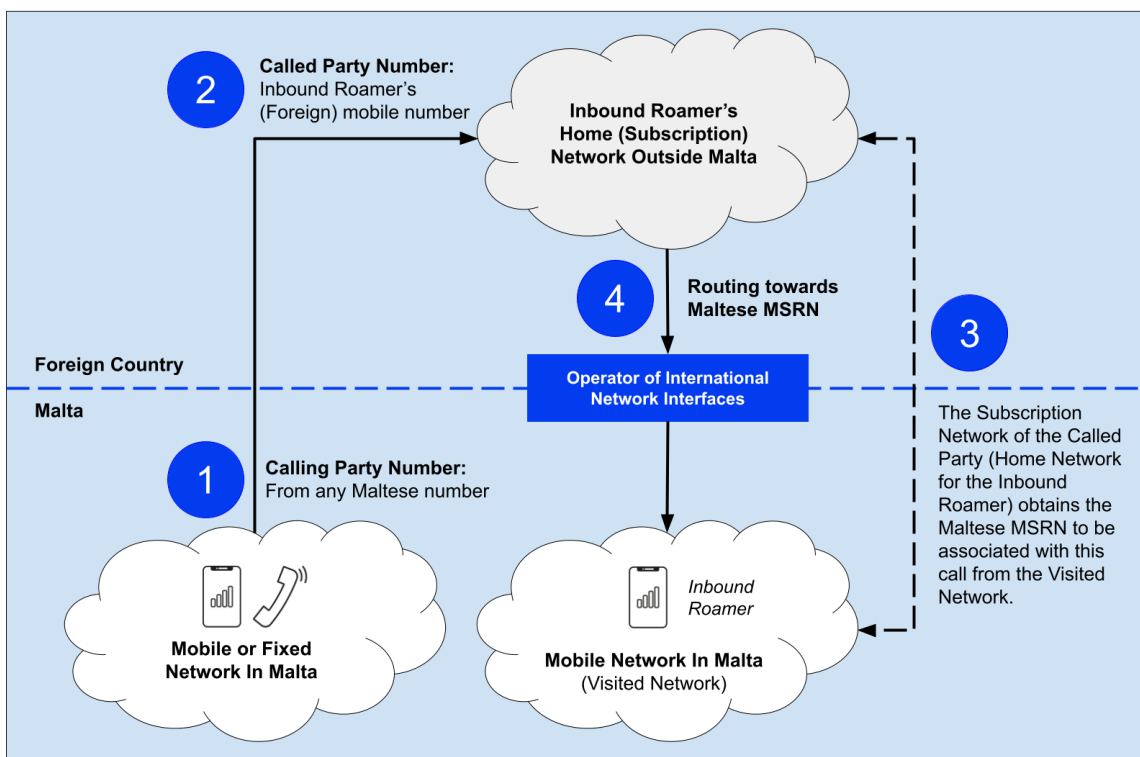


Figure 3 - Simplified flow for Type 'B' calls

The operator of international network interfaces that is first to receive the incoming call in Malta may also be the terminating operator providing the inbound roamer's visited network, but this is not always the case, as international conveyance of calls depends on various factors, such as the commercial agreements established between providers. Thus, before the call can be terminated to the called party, further transit may occur in Malta between local providers.

Type 'C' calls: Call forwarding in specific scenarios where the FTN is a Maltese number

Whilst Type 'C' calls comprise two distinct scenarios, both scenarios include an element of call forwarding which results in calls with a Maltese number appearing to be incoming over an operator's international network interfaces. Figure 4 illustrates the first scenario for such calls.

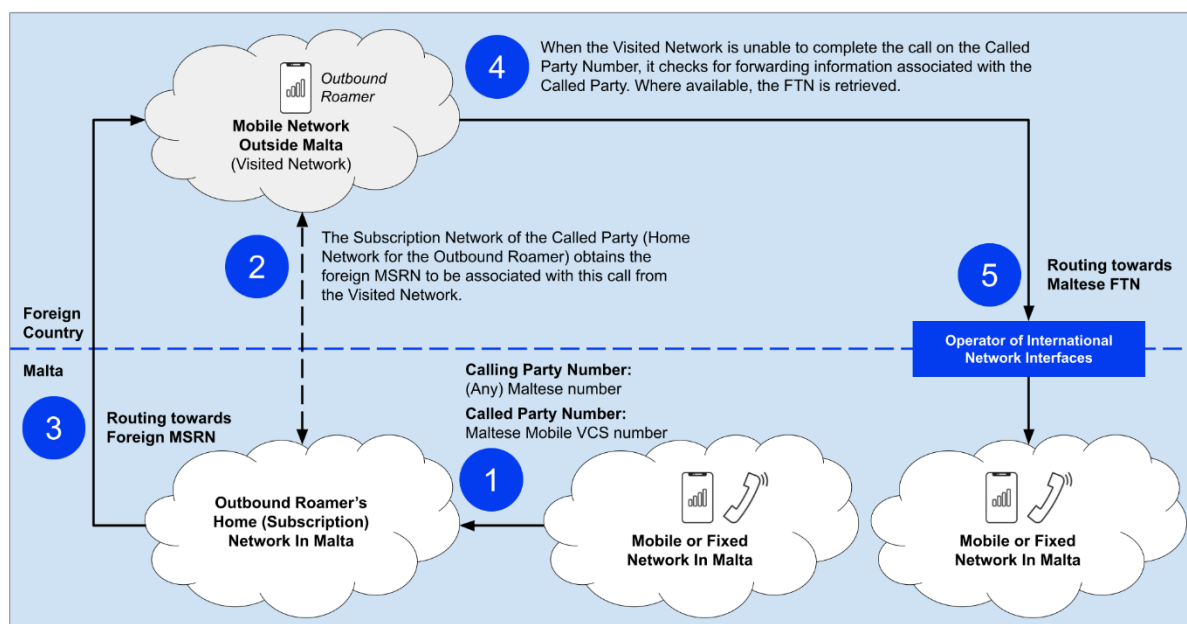


Figure 4 - Simplified flow for Type 'C' (Scenario 1) calls

In this "Type 'C' – Scenario 1", a call is placed by a subscriber assigned a Maltese number towards an outbound roamer (also assigned a Maltese mobile VCS number), and the call would subsequently be late forwarded to another Maltese number. In Step 1, the call with a Maltese CgPN is set up and routed to the called party's subscription network (home network) in Malta. At this point, since the called party is found to be outbound roaming at that time, the home network exchanges signalling with the visited network abroad, as per Step 2, to obtain the foreign MSRN to be associated with the call towards the outbound roamer. Once the foreign MSRN is obtained by the home network, the call is routed towards the visited network so that the latter could terminate the call. At this point, if the visited network is unable to complete the call towards the CdPN for some reason (e.g. outbound roamer is not reachable, busy or not answering), it checks the Visitor Location Register (VLR) for any forwarding information associated with the outbound roamer's profile and the specific reason why the call towards the CdPN could not be completed. Where available, a FTN is retrieved by the visited network (Step 4), and further routing decisions are based on this FTN.

In this scenario of Type 'C' calls, if the outbound roamer had set up late forwarding towards a Maltese FTN for the corresponding reason why the call towards the CdPN could not be completed, the visited network routes the call towards an operator of international network interfaces, as per Step 5. Such routing may involve transiting through other networks before reaching a Maltese operator.

Unless this operator is also providing the subscription network for the FTN, further transit would also be necessary between local providers in Malta until the call reaches the subscription network to be subsequently terminated to the party or service associated with the FTN.

A second scenario is illustrated in Figure 5 below. For “Type ‘C’ – Scenario 2” calls, a subscriber assigned Maltese numbers places a call towards a foreign number which has (unconditional or conditional) call forwarding set up towards another Maltese number.

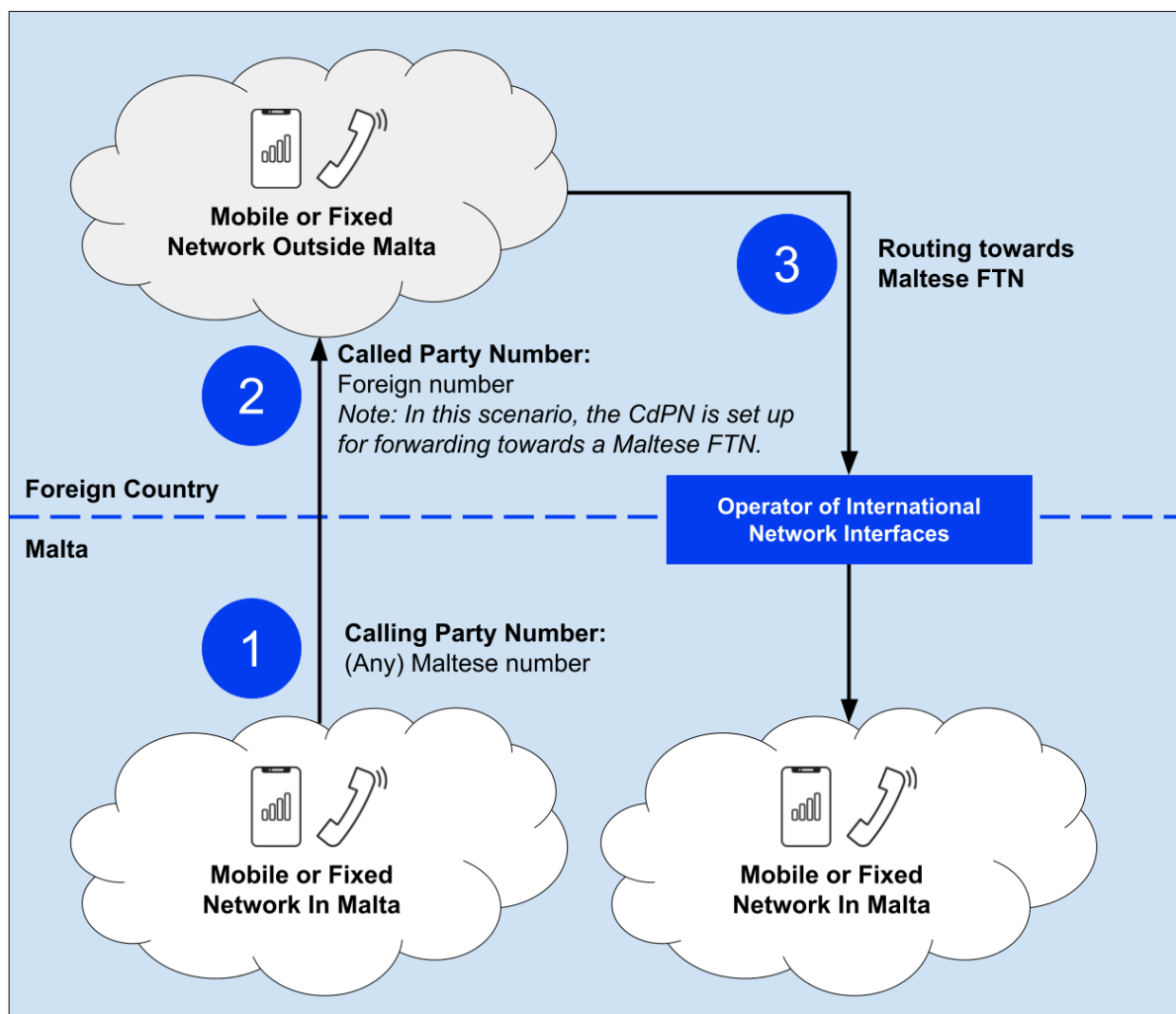


Figure 5 - Simplified flow for Type ‘C’ (Scenario 2) calls

Steps 1 and 2 in Figure 5 above show the call being initiated by the subscriber assigned a Maltese number (Step 1), whereby (based on the foreign number dialled) the call is first routed, and conveyed over international network interfaces, towards the foreign network abroad (Step 2). At this point, since the called party had set up (unconditional or conditional) call forwarding towards a Maltese FTN (number), the foreign network routes the call on a path towards a Maltese operator of international network interfaces for each call in the case of unconditional call forwarding, or when specific conditions involving the called party are met in the case of conditional call forwarding (e.g. called party is not reachable, busy or not answering), as per Step 3. Such routing may involve transiting through other networks before reaching a Maltese operator. Unless this operator is also providing the subscription network for the FTN, further transiting would also be necessary between local providers in Malta until the call reaches the subscription network to be subsequently terminated to the party associated with the FTN.

Annex 2: Candidate Measures in Preliminary Discussions

During the preliminary discussions with the local operators forming part of the ad hoc steering committee, the MCA presented the following 'candidate' measures under **Phase 1**. This Annex also presents the insights gained by the MCA during these discussions.

Candidate Measure 1: Suppress or Replace CLI (except for Types 'A' & 'B' calls)

This measure mandates the **suppression or replacement of the CLI** for all incoming calls over international network interfaces with a national number as CLI, except if either one of the following conditions is met:

- Condition 1: Do not suppress/replace CLI if the CgPN is a national number from an allocated numbering block pertaining to the '4X', '7X' or '9X' numbering range; or
- Condition 2: Do not suppress/replace CLI if the CdPN pertains to a sub-block in use by local mobile network operators for MSRN.

For clarity's sake, when the CLI is 'suppressed', the end-user receiving the call would see "unknown number" (or an equivalent phrase) on a CLI-enabled device. Alternatively, if the CLI is 'replaced', the transmitted CgPN would not be displayed, rather, a replacement number from the Maltese National Numbering Plan would instead be displayed to the end-user. With such a measure in place, the number to be displayed in such 'replacement' circumstances would be specified at a later stage.

Under this measure, fulfilling Condition 1 would safeguard the integrity of the CLI for Type 'A' calls, and spare such calls from CLI suppression or replacement. Thus, calls with national numbers made by outbound roamers or from devices connected to a foreign network would be received by called parties assigned Maltese numbers with an intact and faithful CLI. Similarly, Condition 2 ensures that the CLI is faithfully transmitted to called parties for Type 'B' calls (i.e. calls with a Maltese CgPN received by inbound roamers in Malta).

Operators could also introduce additional rule-based filters in their international network interfaces to identify Type 'C' calls and therefore also prevent CLI suppression or replacement for calls that involved a Maltese FTN. Said that, during preliminary discussions, local operators of international network interfaces informed the MCA that foreign networks send limited, if any, forwarding-related information with incoming calls over such interfaces, which restricted their ability to reliably identify all Type 'C' calls being received. Therefore, if such rule-based filters (to specifically detect Type 'C' calls) had to be implemented, some calls would still not be detectable due to the absent or limited information received.

Depending on the implementation approach adopted, the MCA was informed that calls with CLI suppressed may not be distinguishable from calls reaching Malta with a missing CgPN, and this may impact the wholesale termination rates that may be applied for CLI suppressed calls. In this regard, CLI replacement as an alternative to CLI suppression would address this matter.

In conclusion, it is worth noting that calls would not be *blocked* under this measure. Rather, the key benefit of Candidate Measure 1 lies in its potential to ensure that most known and trusted numbers, (typically fixed VCS numbers), belonging to businesses and other entities would no longer be 'allowed' by operators to appear as the CLI for an incoming call if this was received over the international network interfaces. Rather, such calls would only be terminated with a suppressed (or replacement) CLI.

This measure would thus minimise the effectiveness of scams relying on spoofing such known and trusted numbers to trick the called party into a false sense of security. Furthermore, it could also lead to some consolidation in the messaging adopted for public awareness campaigns. Specifically, awareness campaigns on vishing scams could converge on sensitising the public to be more vigilant when receiving calls that either show “unknown number”, or (if implemented) where the CLI is from the ‘replacement’ numbering range(s)¹¹ dedicated solely to flag potential scam calls.

Said that, during the preliminary discussions, operators were dismissive of the potential benefits of this measure, noting that CLI suppression or replacement would neither justify the effort required to put in place the respective technical intervention, nor the changes needed to wholesale charging arrangements to handle calls with suppressed (or replaced) CLIs. This would apply regardless of whether this measure is adopted on an interim basis, or otherwise.

Candidate Measure 2: Blocking of calls (with some exceptions)

Candidate Measure 2 comprises two variants, namely Variant 2(a) and Variant 2(b), as described below. Both variants mandate the implementation of specific rule-based filters to selectively block incoming calls over international network interfaces where the CgPN is a national number and the indicated conditional exceptions are not satisfied.

Variant 2(a) mandates that calls that correspond to Type ‘A’, ‘B’ or ‘C’ are not to be blocked, whilst all remaining incoming calls with a national CgPN would be blocked. Thus, operators of international network interfaces would be required to check each incoming call within scope against three conditions (corresponding to Type ‘A’, ‘B’ and ‘C’ calls respectively), as follows:

- Condition 1: Do not block if the CgPN is a national number from an allocated numbering block pertaining to the ‘4X’, ‘7X’ or ‘9X’ numbering range; or
- Condition 2: Do not block if the CdPN pertains to sub-blocks in use by local mobile network operators for MSRN; or
- Condition 3: Do not block if the FTN is a Maltese number.

The only difference between Variant 2(a) and Variant 2(b) is that, in the latter case, the check for Condition 3 is not required. Thus, calls with a national CgPN (except where the CgPN is from the ‘4X’, ‘7X’ or ‘9X’ numbering range) that are forwarded towards a Maltese FTN would also be blocked under this variant. The reason why Variant 2(b) contemplates the blocking of a subset of legitimate calls (Type ‘C’ calls) lies in the insights shared with the MCA on the inconsistency in forwarding-related information received by local operators in relation to calls received over their international network interfaces.

In this respect, given the inconsistency in the information sent by forwarding providers, the end-user impact of implementing the check for Type ‘C’ calls (as prescribed under Variant 2(a)), would result in uncertainty around whether calls would be successfully conveyed. It could be argued that end-users could be better off knowing that a specific subset of forwarded calls would be blocked outright, rather than being told that the calls may or may not be blocked. Such certainty would indeed allow end-users to make alternative arrangements as applicable.

¹¹ The Maltese National Numbering Plan would be updated by the MCA to include the specific numbering block(s) from which numbers would be used by providers to replace the CLI of a potential scam call. In time, (and with the support of awareness campaigns), end-users would associate the use of these numbers with a potential scam call, thus lowering the incidence of success for the scammer.

The MCA understands that providing such certainty to end-users could also make it easier for operators to troubleshoot subscribers' issues in this regard.

The primary benefit of Candidate Measure 2, in particular Variant 2(a), is that only the legitimate call types ('A', 'B' and 'C') would be allowed to 'pass through' the international network interfaces, whereas calls that are likely using spoofed numbers would be blocked outright. Such intervention would deny the scammers the possibility to establish the call, and thus reduce the incidence of successful scams. In the case of Variant 2(b), the MCA is conscious that, without any rule-based filter to specifically detect Type 'C' calls, operators would end up blocking these legitimate calls. However, it should also be acknowledged that opting for Variant 2(a) may still result in the blocking of some Type 'C' calls, simply due to the limited information made available by forwarding providers. As noted above, from an end-user's point of view, it may be more practicable to block all Type 'C' calls with a national CgPN outright, (except where the CgPN is from the '4X', '7X' or '9X' numbering range), rather than adopting a measure that induces uncertainty on their conveyance.

Candidate Measure 3: Blocking of calls where the CgPN is a 'blacklisted' number

The premise behind Candidate Measure 3 is to mandate the blocking of all calls where the CgPN is a number that was voluntarily included in a 'blacklist' by the subscriber assigned rights of use for that number. Such a measure would provide certain 'high-risk subscribers' the opportunity to notify the 'blacklist administrator' (defined further down) that any incoming call over international network interfaces bearing such CgPN would correspond to a call with a spoofed number.

In turn, operators of international network interfaces would need to implement specific rule-based filters in their networks to ensure that calls using these blacklisted numbers would be blocked. This measure would result in the blocking of Type 'B' and Type 'C' calls (received over such international network interfaces) where the CgPN is a blacklisted number, and so the subscriber assigned the blacklisted number should be informed of this restriction so that they may use an alternative number when trying to place such calls.

Successfully implementing Candidate Measure 3 would rest on two key aspects, namely:

- a. the technical effort and limits to operate real-time checks for all incoming calls over international network interfaces against the blacklist; and
- b. the effort required to govern the process and ensure coordination amongst all parties.

With regards to point (a), the MCA was informed by local operators of international network interfaces that implementing real-time checks for all calls would considerably slow down the call set-up process, with the extent of the delay increasing in tandem with the size of the blacklist. In simple terms, whilst implementing a blacklist for real-time checks should technically be doable, the (negative) impact on operators' ability to handle calls in an efficient manner would invariably increase as more new numbers are added to the blacklist. In this respect, a critical success factor for Candidate Measure 3 is to ensure that the blacklist is limited to a manageable size.

The above insights also shed light on the importance of establishing the right framework for governance and coordination amongst all stakeholders involved, as per point (b). This is particularly critical given the technical constraint requiring the strict management of the size of the blacklist. Thus, as a minimum, a governance and coordination framework would be needed to address the following aspects:

- a. determination on who should take on the role of the 'blacklist administrator' and thus be responsible for managing the blacklist (i.e. inclusion/removal of numbers, dissemination as needed, etc.);
- b. clear definition of what constitutes a 'high-risk subscriber', particularly to determine who would be permitted to propose numbers for inclusion in the blacklist;
- c. guidance on how to propose numbers for inclusion in or removal from the blacklist;
- d. clear rules on what factors are to be considered when determining whether a proposed number should be included in or removed from the blacklist; and
- e. guidance to all providers to ensure access to the updated blacklist (either on a real-time basis, or through frequent updates).

Candidate Measure 4: Blocking of calls where the CLI is either a number from unallocated numbering blocks or from inbound-only sub-blocks

Candidate Measure 4 would require operators to implement a real-time check for incoming calls over international network interfaces to ensure that the CgPN is not a number from a predefined list identifying either numbering blocks that are unallocated (e.g. the entire block starting '6X') or numbering sub-blocks that were allocated to providers solely for 'inbound-only' purposes¹². In turn, if the CgPN belongs on this list, the call would have to be blocked. This check could possibly also be extended to cover all incoming calls (i.e. even those incoming over national network interfaces).

In contrast with Candidate Measure 3, this measure would not require an elaborate governance or coordination mechanism beyond the initial implementation phase, coupled with timely updates to the list as needed (e.g. where new sub-blocks are designated for inbound-only purposes). In any case, such timely updates are not expected to be frequent.

If Candidate Measure 4 had to be implemented, the MCA acknowledges that operators could come across the same technical constraint mentioned in respect of the blacklist facility (Candidate Measure 3). Indeed, the technical constraint related to the size of the blacklist would also apply with regards to the size of the list of numbering blocks/sub-blocks to be checked, in real-time, under this measure. In fact, operators confirmed that blocking whole ranges (e.g. a 1-digit prefix, such as '6X') would be less taxing on call set-up time, and would therefore be more ideal, as opposed to checking the CgPN against a list of numbers or more granular sub-block prefixes (e.g. a 3-digit prefix, such as '200X XXXX') representing specific unallocated or "inbound-only" sub-blocks. The MCA therefore recognises that the successful implementation of Candidate Measure 4 would rest on striking the right balance between the extent of granularity to impose, and the risks associated with not blocking certain CgPN despite being from unallocated numbering blocks and/or from inbound-only sub-blocks.

¹² During the preliminary discussions, the MCA informed the operators to consider, at the time, that the list of 'inbound-only' numbering sub-blocks would comprise up to 10 sub-blocks granular to 5-digits (i.e. 1,000 possible numbers per sub-block); and up to 5 sub-blocks granular to 6-digits (i.e. 100 possible numbers per sub-block).



MALTA COMMUNICATIONS AUTHORITY

 (+356) 2133 6840
 info@mca.org.mt
 www.mca.org.mt
 Valletta Waterfront, Pinto Wharf,
Floriana FRN1913, Malta