Good practice guide to help prevent misuse of sub-allocated and assigned numbers

The full list of consultation questions is set out here.

1. Do you have any comments on the suggested measures set out in Section 3? Ofcom states that - *We aim to disrupt scams by making it harder for scammers to use communications services to reach consumers - When contacting consumers by phone, scammers often claim to be from legitimate organisations as part of their method of tricking their victim into providing personal details or making a payment. Having access to a valid phone number adds to the scammer's perceived legitimacy.*

Ofcom has good intent with these aims but perhaps misses a point - that a vast number of scams are intended to get the victim to call the fraudster back. In your examples this MO is not mentioned but we are all aware of thousands of victims having called an 033xxx or a 0203xx number believing it was 'the bank' or a 'delivery company'. Scammers / fraudsters are attracted to what are essentially virtual numbers such as Number Translation Services supplied by Telcos that specialise in providing DIDs. (direct inward dialling).
The problem with respect to this draft Guide is - most of it is limited to Business clients. But the DIDs obtained by scammers / fraudsters are not being supplied to businesses rather they are supplied to clients who present as Consumers. There are dozens of websites offering anyone with a credit card unlimited access to a choice of 087, 084,03 etc and also very importantly millions of Landline numbers across the country – virtual landlines. Simply choose an 0203xxx number, provide a phone number (mobile) to deliver the calls to, give card details – job done and that's it! These all operate technically in the same way as a Number Translation service, i.e. they all route / deliver / divert to another phone number provided by and belonging to the scammer / fraudster. Most often the 'deliver to number' is a mobile number. This is why they are so attractive to scammers.
The ONLY checks that are made when placing an order for a DID is – a valid credit / debit card! The Good practise guide needs to include ALL of these product offerings irrespective of the type of client Business / Consumer. If not the scammers will simply (as they do right now) present themselves as individuals / consumers and avoid these KYC checks being made. It is to be suspected that the providers of these DIDs will not want to make these checks unless the Guide pushes them - it needs to be extended to Consumer for provision of these DIDs products.
On a similar note there is a service called SKYPE NUMBER which is also used for scams that require victims to call to the fraudster, especially when the scammer lives abroad. Ofcom should consider if the KYC part of the Guide should extend to Skype Number – it already will with regards to reported misuse incidents.
An individual SKYPE NUMBERs will deliver PSTN phone calls to the associated SKYPE app anywhere in the World. The Skype app is free and therefore requires minimal KYC, a Skype Number can be added to the App at a cost of £5/month paid by card. Very attractive to fraudsters who operate thousands of miles from the UK but want to have a landline number in say London or Glasgow which they can answer on their Laptop! Of course unlike DIDs this does not involve delivering the incoming calls to a phone number because the calls are delivered by the relevant UK telephone networks over VOIP directly to Skype and then out to the associated

Skype app. Because of the freedom given fraudsters / scammers based overseas find these UK numbers (mostly) Landline numbers very useful.
FYI - Due to German regulations [also France, Switzerland, Brazil and S.Korea], when you request a Skype Number in Germany you will be required to verify that you are a German resident in the same area where you would like to purchase a number. After you complete the online form you will be given the selected Skype number. You will then have 14 days to verify your address.

2. Have you used any other due diligence checks that you think would be beneficial if adopted across the industry?

Experience shows that test calls made to these numbers – shortly after provision often reveals the true nature of the scam.
If a DIDs provider was required by the Guide to ascertain how the client intends to answer incoming calls – i.e "Village Bakery" or "IT services". When test calls are then made a few hours later (and again 12 hours later) if the calls are answered "HSBC"or "Microsoft" then it can reveal the scam very rapidly. But non of this happens if the 'Consumer' clients are excluded from the Guide.
This testing approach would similarly work with regards to SKYPE NUMBERs which are also used for scams require victims to call to the fraudster. SKYPE NUMBERs are answered via the SKYPE app anywhere in the World. Very attractive to fraudsters who operate thousands of miles from the UK but want to have a landline number in London or Glasgow!

3. Do you have any comments on the suggested measures set out in Section 4?

In order to minimise the risk of providing a virtual number (DID) to a scammer which will then be used for victims to call. It would be of great benefit if other DIDs providers were to share details within the Industry relating to the Deliver to numbers which have already been linked to scams / misuse / fraud. i.e. Share details of the mobile phone numbers that the scammers used. If one DIDs provider has blocked a scammers virtual numbers that DIDs provider will clearly also block the associated mobile number on their own platform. Why not share that detail across industry in order to disrupt the scammers more efficiently.

5. Do you have any comments on the suggested measures set out in Section 5?

Clearly when it comes to 'Misuse' Ofcom recognise the importance that the Guide should apply to all types of client both Business and Consumer. This is good.
For the benefit of the Mobile networks perhaps Ofcom could give some examples where it feels the use of a Mobile involved in Scams / frauds could and should be disrupted. Some mobile networks seem to be reluctant to take action even when presented with evidence of involvement in scams.
In the DIDs scenario Ofcom could indicate that if the scam number was 'delivered' to a mobile number on a permanent basis that is sufficient grounds for a Mobile network to disrupt that mobile number. If the evidence of DID misuse of say an 0203xxx number is sufficient to disrupt that 0203xx number. Then the fact that this number will not function without its associated 'deliver to number' - the mobile – in such instances the associated mobile network provider would also be protecting victims of scams by disrupting that mobile number.