Q1: Do you agree with our definition of Information, connection and/or signposting services (ICSS)? If not, what alternative would you propose?
Yes.

Q2: Do you agree with our description of how ICSS operate? Are there other variants not covered in this section?
Yes. The description provided in the consultation document broadly covers the various types of ICSS operating models.

Q3: Do you agree with the distinction we are making between the connection and signposting aspects of ICSS on the one hand and directory enquiry services on the other? If not, why not?

Yes, it's an appropriate distinction because Directory enquiry (DE) services are not exclusively linked to a single service or set of services. Consequently, users of government services are better able to make the distinction between the DE service provider and government service providers and their affiliated bodies. As a result directory enquiry services do not present the same potential for reputational risk to government that ICSS providers do. Further, users of directory enquiry services are far more likely to be aware that there is a cost for the "look-up" and connection service they receive from a DE provider while this is often not the case with many ICSS providers.

Q4 – Do you agree with our assessment of consumer harm in relation to ICSS? If not, why not?
Yes.

Q5 – Is there other evidence of concerns and/or harm that you are aware of and which have not been referred to in this section? If so, please provide them and any evidence that substantiates them.
No. The scenarios described in the case-studies and the summary outlined in paragraph 2.14 covered our concerns about the harm that ICSS providers, who present misleading information, cause to users of government services.

Q6 – Do you agree with our assessment that ICSS carry a level of risk which meets the threshold for a prior permissions regime? If not, why not?
Yes. The two main reasons for our position are: (1) the protection of users of government services and (2) the misleading activities of some ICSS providers, most of whom advertise their services online, has the potential to cause users of government services to distrust digital channels. This could have a disproportionately negative impact on the ability of legitimate government service providers to offer these services via digital channels and in so doing, militate against the UK government's commitment to widening access and delivery of public sector services to include faster, more convenient and cost effective online channels.

Q7 – Do you agree with our proposed exemptions from a requirement to seek prior permission? If not, why not?

Yes. Further we believe that, should the proposal be adopted and awareness of the conditions under which ICSS providers operate increase, it will much be easier for services/product users to authenticate ICSS providers via PhonepayPlus, Charity Commission or the legitimate service provider. This will in turn, increase levels of trust with regards to the services in question.

Q8 – Do you agree with this assessment and PhonepayPlus' proposed conditions around Search Engine Marketing (SEM)? If not, why not?
Yes. In keeping with the UK government's commitment to making government services "Digital by Default" in order to offer more convenient, efficient, and effective public services, many users of government services will be encouraged to access services online, possibly for the first time. A good proportion of these first-time users of online services will be those who were previously digitally excluded. It is highly unlikely that they will be sufficiently aware of how SEM works and as such will be particularly susceptible to misleading Search Engine Marketing practices. The proposed conditions related to SEM will protect these vulnerable stakeholders in particular.

Q9 – Do you agree with the need to require the inclusion of specific wording in SEM results as displayed to the consumer on-screen in search engine results that states "This is a premium rate telephone service"? If not, why not?
Yes. Transparency about the cost of the service will help people to make informed decisions about the ICSS service and whether or not to use it. This also allows service users to assess whether the cost of the ICSS service genuinely represents value for money.

Q10 – Do you agree with this assessment and PhonepayPlus' proposed conditions around promotion of ICSS? If not, why not?
Yes, in particular the condition set out in 4.18(d) i.e. when personal and/or confidential details are requested from users, the ICSS provider must inform them that it is acting in an intermediary capacity and not as an agent of the actual service provider. There have been situations where users of government services have unwittingly provided personal or confidential information to third-party organisations believing they were interacting with a government service provider. In addition to the distress of discovering they have been charged additional fees for a service that government provides for free or at a lower cost, there is also a concern that their confidential or personal information is in the hands of third-party organisations whose operating procedures are not always clearly stated or reliable.

We agree that it is important that users of government services are made aware of the definitive source for information about or access to the services they are seeking and we believe that providing a website address fulfils this requirement. This will also help to ensure that users are pointed in the direction of the most up-to-date contact information for the services they are seeking.

Q11 – Do you have any views on whether condition B ii) should be applied to all ICSS, or whether an altered condition, as outlined above, should apply only to connection Review of Information, Connection and/or Signposting Services PhonepayPlus Page 38 of 47 and signposting services which can prove they are not used mainly by vulnerable people and link to genuinely hard to find numbers? If so, please provide them, and any evidence which supports them.
In our view, condition B ii) should not be applied to *any* ICSS providers. This is because requiring them to provide the helpline details of the actual service provider undermines their business model and is likely to result in affected ICSS providers widening their activities beyond "connection and signposting services" to incorporate services related to an "information advice or assistance service" rather than significantly changing their practices to protect users. This is because providers of "information advice or assistance service" will only be required to provide "the phone number or web address where the consumer can obtain the information, advice or assistance..." (see 4.18 b iii). In other words, we believe the underlying objective for the proposed condition is unlikely to be achieved. It is our view, that the inclusion of a website URL

would be sufficient in all cases and removes the perverse incentive described here. Further enforcing penalties for violation of condition B ii) would be complicated by the fact that there is currently no consensus on what constitutes a "vulnerable" consumer or "hard-to-find" number.

Q12 – Do you agree with this assessment and PhonepayPlus' proposed conditions once a consumer has dialled an ICSS? If not, why not?
We are broadly in agreement with this assessment of the models by which ICSS providers deliver their services (as set out on pages 28 - 30) and with the "prior permission" conditions you've outlined in order to tackle them. However, we were concerned that condition (g) could introduce the unintended effect of extending the length (and therefore cost to service users) of the call under the guise of informing users how their "data will be stored, retained or further used". We would propose that the wording would be revised thus:

"Where the consumer is asked to supply secure personal and/or confidential details, then they must be clearly informed that their details are being provided to a third party, and not the organisation they wished to contact. In addition, where such secure data will be used to log into a consumer's online account in order to undertake any action on their behalf, then consumers must be clearly informed of this and that they could perform these actions themselves at no cost. They should also be advised that information about how this data will be stored, retained or further used is available on the ICSS provider's website." This will require that one of the conditions for permission would have to be that the ICSS provider must include this information on their website.

Q13 – Do you have any views on whether condition B should be applied to all connection and signposting services, or whether an altered condition, requiring that the consumer is given the website of the organisation they are looking for rather than the actual number, should apply to connection and signposting services which can prove they are not used mainly by vulnerable people and link to genuinely hard to find numbers? If so please provide them, and any evidence which supports them.
Yes. For our rationale, please see our response to question 11 above.

Q14 – **Do you agree with this assessment and PhonepayPlus' proposed condition where an ICSS collects personal and/or confidential data from consumers? If not, why not?**
Yes. However, we have some concerns about the implications of providing users with information about the ICSS provider's intended use of such information during the call could have on the length and therefore cost of the call. We would propose that this information be provided at no cost at the start of the call and not at the premium call rates.

Q15 – Do you have any thoughts on whether a bond is necessary? If so please provide them, and any evidence that supports them.
No - we have no thoughts on the need for a bond

Q16 – Do you agree with our impact assessment? If not, why not?
Yes, as all four factors have the potential to affect our users' confidence in accessing government services particularly via digital channels.