Dear reader,

After reading the draft G*uidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 1.0,* I am extremely worried about the processing of silent party data.

As the draft guidelines describe in the example of paragraph 44, silent party data can be processed without this party's awareness or consent. Because financial data can contain highly sensitive and private data – such as medical expenses and indicators of wealth – combined with the fact that the silent party is unaware of their data being processed, extra protections must be built in.

Performing the contract with the payment service user (as described in 47) is not proportional to the infringement of the silent party's rights. It is unreasonable to expect anyone's personal data is acceptable collateral damage for someone else's convenience features.

These concerns are extra important because of the potential of payment service providers to reach significant market share – for example, in the realistic scenario where Apple or Google includes PSD2-services in their mobile platforms. The more users consent to sharing their data, the less control silent parties have over their information, and these (or other) corporations gain a bigger and better picture about all silent parties that never wanted to share their data to begin with. Although this kind of further processing is limited according to the draft guidelines, companies of this scale have shown time and time again they cannot be blindly trusted.

Even with proper oversight, data breaches are a serious threat – even for the "digital giants". If not malice, then incompetence or sheer bad luck can lead to breaches of silent party data. Massive hacks in the past, such as the iCloud hack in 2014 or the more recent breach of confidential materials from CPU-maker Intel, have shown that no data is ever completely safe. By providing access to silent party data, their privacy is put at risk without their knowledge, consent, or even the slightest form of influence: it would force privacy conscious individuals to go back to a cash only life, which is practically impossible this day and age.

Luckily, prevention is an option. Silent party data should be anonymized. Imagine party A, B and C use services from the same provides, and they all have transactions with silent party S. Transactions with S should not just legally, but also technically be impossible to link to one individual. Names and account numbers of silent parties should not be accessible to the payment service provider – only transaction dates and descriptions.

So long as payment service providers have the technical access to silent party data, it's just a matter of time before their privacy is breached. When that happens, it doesn't matter whether it's through malice or incompetence: the genie is out of the bottle and there's no way back.

The only way forward is to establish far reaching safeguards for silent party data.

Thank you for your consideration.