Privacy Vaults Online, Inc. d/b/a/ PRIVO, an authorized Safe Harbor provider under the Children's Online Privacy Protection Act ("COPPA") hereby responds to the Commission's "Questions on the Parental Consent Method" in connection with the application for approval of parental verification method filed by Imperium (the "Parental Verification Method Application") as follows:

1. Is this method already covered by existing methods enumerated in Section 312.5(b)(1) of the Rule?

Yes. As presented in Imperium's initial Parental Verification Method Application dated August 12, 2013, the ChildGuardOnline service consists of these elements: (1) An email notifying the parent of the child's effort to register with a site or app, the URL of that site or app, and the parent's right under COPPA to review and delete the child's information; (2) A verification of parental identity via the last four digits of social security number; (3) A back-up method of verification, for use in the event that the social security number check is not successful, which method consists of knowledge based authentication ("KBA") via "out of wallet" challenge questions; (4) some undefined anti-fraud measures to assure that the same identity is not "over used," and (5) a parental portal. Element 1 is a process that all sites and apps use to comply with COPPA and presents nothing new for the Commission to approve. Element 2 is already on the Commission's list of approved methods and does not need Commission approval to be used. Indeed, PRIVO has offered this method of verification almost a decade. As a matter of fact, all of the existing safe harbors have approved online operators who use this method. Element 3 is widely used in the online verification space, which Imperium notes. It might be more widely used if it were less intrusive and annoying to the end consumer

and not cost prohibitive for the operators. Element 5 is a centralized consent management tool that also appears to aggregate data. There are other centralized consent management tools in existence and in development, including PRIVO's. The Commission has been aware of this concept since 2004 and recently encouraged their development to simplify the COPPA process for parents and operators. But, the Commission does not require that operators get approval to use such a tool. Therefore, there is simply nothing in the Application that is appropriate for Commission approval.

However, Imperium's September 17, 2013 written responses to the Commission's telephone inquiries, indicate that there may well be alarming deficiencies in the Application that the Commission should address. For example, it appears that, before attempting to confirm the parent's identity via the parent's social security number, Imperium will first conduct a person search to see if the name, address and DOB of the parent match. Once that data has been pulled, Imperium must then ask the parent to self assert the child's address and age. Only after all of this, Imperium asks for the last four digits of the parent's social security number.

In addition, Imperium's September response indicates that Imperium will also use geographic location technology to strengthen its KBA process. It is difficult to determine, without seeing the precise questions that Imperium will pose, how also gathering geo-location data will help establish a link between the child and the purported parent. The parent-child scenario is different from the other scenarios in which Imperium has used geo-location data to support its KBA. It would seem that one way parent geo-location data would be helpful would be if Imperium also collected the child's geo-location data to be able to compare it. This collection violates COPPA if done without parental consent. Moreover, it is of limited value

where it shows that the parent and child actually are in the same location. This could mean that either the parent is with the child, or that there is no parent at all, just a fictitious identity created by the child.

Further, the notification that Imperium describes as being sent to the parent, which would include a URL link for the parent to review the site, does not appear to contain the required information required under the Commission's rule and suggests that Imperium does not have a full understanding of the requirements of COPPA, yet seeks to hold itself out as a COPPA solution provider. It would reasonably be expected that a service that delivers COPPA compliant solutions would have standards that apps and sites that use the service must adhere to. Yet, there is no mention of this in the publicly available materials regarding the Application.

As another example, the signup process that Imperium describes implies that the only information collected from the child is the parent name and email address. Industry has for a decade been collecting the child's first name and the parent email because the parent name is of no use to the site in advance of getting consent. It does not aid in the delivery of the email. In fact, it would likely alarm a parent if it said "Denise Tayloe your child requests your consent". The acceptable COPPA norm is to use "Parent, child first name requests your consent." Note that the child's first name is critical here. Otherwise the parent will not be comfortable that the email is not spam, and if the parent has more than one child, will not know which child the parent is permissioning to the site or app. It is simply too much to ask of a child to provide the parent's name and email address all at the same time.

The discussion around the operators "ping[ing] a web service to confirm that the furnished user name has been approved" raises many questions as well. It is not clear if the user

name is merely a display name and if the parent is made aware that the user name will be displayed to the public with or without the parent consent. It is not clear if Imperium is creating and managing the child account user name, and if it does, whether the system insures that linking cannot take place across services using the ChildGguardOnline service, as required by the NSTIC Guiding Principles and best practices in the identity space.

Indeed, the flow of information is not well described at all. For example, there is no explanation as to how the site or app that uses the service will show the parent the information it has collected. There is just a simplistic statement that Imperium will let the parent know of its right to find that information out. It does not describe if a parent can visit the operator's site to manage the child account and to view or delete the information collected, or if the parent must come back to the ChildGuardOnline site to do so. The Application does not discuss how the operators will get the contact data they need to communicate with the child. The information provided suggests that Imperium will process only the permissions centrally and that the child will share his or her contact data directly with the site, but this is far from clear.

Finally, the unspecified anti-fraud measures raise questions. There is no discussion concerning what these measures might be or how they might impact parent and child privacy. In the absence of such an explanation, it seems likely that Imperium will have to develop a large database of parent and child identities in order to identify "over use" of identities.

As a result of the limited information provided in the Application and the additional questions that limited information raises, it is hard to fully assess the Application. However, it is clear that the Application does not present any new method requiring Commission approval. Rather, in this Application, the Commission is again confronted by an Applicant seeking to

cobble together a number of methods, in this case ones that have already approved by the Commission or by Safe Harbors, and then secure the Commission's blessing allowing it to market a proprietary method. Again, the applicant does not take any responsibility for vetting the sites and apps that will use the tool to determine whether it is appropriate for their services and that it is being used in a COPPA-compliant manner. Indeed, in the case of Imperium, it appears that several aspects of the service will not comply.

2. If this is a new method, provide comments on whether the proposed parental consent method meets the requirement for parental consent laid out in 16 CFR § 312.5(b)(1). Specifically, the Commission is looking for comments on whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

As noted, many questions about what the method really involves exist and have not been clarified by the information that is publicly available concerning the method. The overriding difficulty with the method, however, is that it forces all parents and children to use a very high level of verification, even when such a high level is not required. The Commission's COPPA rule incorporates a sliding scale of verification depending on the risk level involved in the activity the child seeks to engage in. Under Imperium's method, though, a parent would have to disclose a great deal of information, potentially including social security number and geo-location data, simply to allow a child to sign up for a generic newsletter. Not only is this overkill, but it seems calculated to generate a large data store of information more than protect child identities. Without knowing what Imperium's business model is, the Commission cannot

be sure that more information is not being collected in the name of protecting child than can be justified.

3. Does this proposed method pose a risk to consumers' personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this method?

As outlined above, there are many unanswered questions in the publicly available materials about how the service will work, but a reasonable analysis of it raises many privacy alarms. By way of example, in the Aristotle safe harbor proceeding, the Commission established privacy safeguards by requiring that Aristotle separate its databases. At a bare minimum, that safeguard should be required here as well. Similarly, in the safe harbor process, applicants must demonstrate what their business model is to show that they can stand up a resilient service and to surface any conflicting uses that data collected might be put to. For these reasons, and all those discussed herein, the Commission's verification method consent process is not appropriate to address methods such as the one advanced in this Application.

Therefore, PRIVO submits that the instant Parental Verification Method Application is completely inappropriate for the Commission's verification method approval process. It does not present a new method, so the Commission would simply be validating a particular applicant's proprietary business method. KBA is already a widely used method, and could be added the Commission's list of approved methods without the entanglements of a specific proprietary methodology. Moreover, very serious questions remain from the publicly available materials as to the reliability, security and intended use of the data collected via this proposed method.

Respectfully submitted,

PRIVACY VAULTS ONLINE, INC. d/b/a PRIVO

By: ___/s/_____
Denise Tayloe, CEO

Dated: November 4, 2013