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 AssertId (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?

As presented in AssertId's Parental Verification Method Application, the AssertID process contains six (6) elements: (1) A process for parental notification of consent-request; (2) A process of presentment of consent-request direct notices to parents; (3) A process for recording and reporting a parent's response to a consent-request to the Operator; (4) A process for recording and reporting a parent's request to revoke consent previously granted and to have their child's personal information deleted; (5) A process of verification of the parent-child relationship; and (6) A process to ensure that only a parent of the child for whom consent is being requested can access and respond to such requests. Elements 1, 2, 3, 4, and 6 constitute a centralized consent management tool. There are other centralized consent management tools in existence and in development, including PRIVO's. The Commission has encouraged their development to simplify the COPPA process for parents and operators. Accordingly, PRIVO submits these aspects of the AssertID Parental Verification Method Application do not require Commission approval.

The sixth element of the AssertID process involves leveraging "advances in the science of Social Network Analysis" or SNA, and seeks approval for a proprietary, patent pending social

verification process. The area of social verification is just developing in the identity space. Governments including the EU and the US are debating what social verification is, how to define it, whether it holds the potential for streamlining identity online, and if so, how to regulate it to protect consumers. In considering whether to accept some form of social verification as a reliable parental consent verification method, the Commission should not tie its decision to a proprietary method. Ultimately, the Commission, along with other governmental bodies such as the National Strategy for Trusted Identities in Cyberspace ("NSTIC"), may be called upon to define exactly what social verification is and establish the parameters within which it must operate to meet the NSTIC Guiding Principles and be accepted among the United States' global trading partners. Choosing a proprietary method at this early stage risks preempting this much larger policy discussion that is taking place on the global stage and in all aspects of the emerging identity ecosystem for trusted transactions in cyberspace. Approving a single method in the COPPA space risks chilling other innovators in the space and potentially involves the Commission in reviewing and monitoring each iteration of the AssertID process to assure that it remains in compliance with the Rule.

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.

PRIVO submits that the type of social verification and vouching set out in the AssertID Parental Verification Application, without more, does not meet the requirements of full parental

verification required when an online service will share children's personally identifiable information with third parties such as ad networks, or permit children to disclose that information, such as through chat or other features. The AssertID methodology relies on individuals in the asserted parent's social network to vouch for the parent's identity. PRIVO submits that at this time, such vouching is not sufficiently reliable to be accepted as a method of full parental verification. As the Commission is aware, many children under 13 have established social media accounts by falsifying their age information. Many of these accounts have been active for years and are likely to be among some of the most active users of social media services. As a result, these unverified and grossly age-inflated accounts will appear to be credible social profiles with the result that minors will easily be able to vouch for other children under 13.

AssertID's process was previously described in its United States Patent Application for Method and System for On-Line Identification Assert (the "Patent Application"). In the Patent Application, AssertID identified a number of scenarios in which users could subvert the AssertID social verification process, such as a motivated child molester, a conspiracy among multiple criminals, friends spoofing the system to help other friends, and friends creating false accounts "just for fun."[1] To counter these scenarios, AssertID proposed enforcement measures with corresponding punishments designed to reinforce the social norm of creating truthful profiles and responding to verification requests honestly. Among the deterrents to spoofing and

[1] Patent Application at [00120-00123].

circumvention that AssertID proposed to use are credit checks on all users and random verifications of user information against credit reports.[2]

AssertID's Patent Application also describes the methodology by which trust scores will be established. It notes that the highest score is 100, but that no one can achieve a score greater than 50, unless they become a "trusted anchor."[3] The application states that trusted anchors are important to the development of the trust ecosystem necessary for SNA to work. Where an individual does not have a significant online social presence, their attributes can be validated at a much higher level of confidence by using other verification processes such as verifying against credit rating and other online "trusted" databases.[4] Once verified, these trusted anchors then "seed" the trust ecosystem to increase trustworthiness of the SNA process.

However, the AssertID process set forth in the Parental Verification Method Application does not indicate that AssertID will include these additional enhancements that the Patent Application indicates are necessary. While social verification may hold many possibilities, it does not appear to have matured at this time that one method, and an incomplete method at that, should be established by government fiat.

Finally, PRIVO notes that in the Parental Verification Method Application, AssertID disclaims all responsibility to assure that operators using the method, if approved, do so appropriately. As stated previously, the social verification method set forth in the Parental Verification Method Application may be as reliable or more reliable than the currently approved Email Plus method, but it does not rise to the highest level needed by many operators. The

[2] Id. at [00124].
[3] Id. at [00131].
[4] Id. at [00114-00116].

availability of an "FTC Approved" consent method that does not require operators to assess and reassess their information collection and use practices could well lead to a false sense of security for parents and for operators who may believe that by using the AssertID process, they are COPPA compliant. The trend in the identity space, led in the United States by NSTIC, is to establish trust frameworks that (1) clearly lay out the policies to which identity providers, relying parties and consumers must adhere and (2) audit those parties' compliance with the established polices. These frameworks must follow the guiding principles of NSTIC, which include, easy to use, secure and resilient, interoperable and privacy enhancing -- not privacy neutral or less, in order to be approved for use for instance with our own government. To suggest that an identity and consent management service such as AssertID would not take any responsibility for the relying parties' compliance with the policies it purports to uphold, in this case COPPA, would be going backwards from what is currently being offered and what others in the industry are working towards.

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?

The AssertID process as outlined in the Parental Verification Method Application poses substantial risks to consumers' personal information. While the Parental Verification Method Application states that the AssertID process avoids the need for parents to release sensitive credit card or government issued identification information, they must give up a considerable amount of other personal information. First, in establishing their "digital identity," parents self-assert attributes including their profile picture, age and location, much of which can be hidden in social profiles, but which will have to be unveiled to use the AssertID method. Second, this newly

created AssertID will be verified by direct verifiers and the verifiers of these direct verifiers. In order for these peer verifications to be of any value, AssertID will need to know something about the direct verifiers, and then in turn about the indirect verifiers. It does not seem possible to give sufficient disclosures to the parent, its direct verifiers, and the vastly wider circle of indirect verifiers of the consequences of their participation in the vouching process, or even that they are involved in the vouching process. Third, the Parental Verification Application describes the trust score as "dynamic" and "continuously updated." To function in this way, then, the AssertID process must involve considerable data aggregation and tracking of the parent, and likely of the child, direct verifiers and indirect verifiers. At a bare minimum, the FTC must assure that the databases that AssertID will amass are subjected to strict data protection and use controls and that all parties are clearly and fully educated with regard to these practices so that they can exercise truly informed consent in agreeing to establish an AssertID.

Finally, to the extent that AssertID will use any of the enforcement mechanisms or the trusted anchor process described in its Patent Application, either at launch or at a later iteration of the product, a great deal more consumer data will be gathered than any of the existing approved parental verification methods. It is antithetical to the NSTIC Guiding principles and tenants underlying COPPA itself to require that a parent establish a social identity and give that identity over to a third party in the name of protecting their child's privacy.

It is noted that AssertID proposes to offer its basic service to consumers and operators for free. The only two revenue streams that are readily apparent to make this model economically feasible come from the premium services and the aggregated data in the AssertID databases. The Commission recently imposed upon operators the requirement to know the information practices

of plug ins, analytics providers and the like precisely because it discovered that these were offered for free because of the value of the data they received in return.

In sum, if the Commission is going to move forward with the approval of any social verification method, it should do so on the basis of a broader rulemaking proceeding involving the full panoply stakeholders in the identity space. While the Parental Verification Method Application may well serve as an important catalyst in the coming discussion, it is not appropriate for the Commission's process to be used to validate a proprietary business method, and the parental verification method put forth is not at this time sufficiently reliable or privacy enhancing to warrant approval as submitted.

Respectfully submitted,

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

By: ___/s/_____
Denise Tayloe, CEO

Dated: September 20, 2013