IMPERIUM

September 17, 2013

Kristin Cohen, Esq.
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Via Email and Federal Express

Re: Responses to FTC Questions Regarding Imperium Pursuant to COPPA Rule Section 312.12(a) for Approval of Parental Consent Method Not Currently Enumerated in Section 312.5(b).

Dear Ms. Cohen:

Pursuant to Section 312.12(a) of the FTC's rule (the "Rule") promulgated under the Children's Online Privacy Protection Act of 1998 ("COPPA"), Imperium, LLC ("Imperium"), has submitted an application for approval for its ChildGuardOnline™ service ("ChildGuard Service") as a parental consent mechanism not currently enumerated in the Rule. Imperium's application, originally submitted on July 1, 2013, and revised on each of July 22, 2013 and August 12, 2013, was posted for public comment on the FTC's website on September 9, 2103.

Following our telephone conference on September 11, we received questions via email from you on September 12 regarding specific aspects of the knowledge-based authentication ("KBA") method that the ChildGuard Service uses as a backup for parental identity verification in the event that the information supplied by the parent in the primary method (name, address, date of birth and last four digits of social security number) is not verified.

Responses

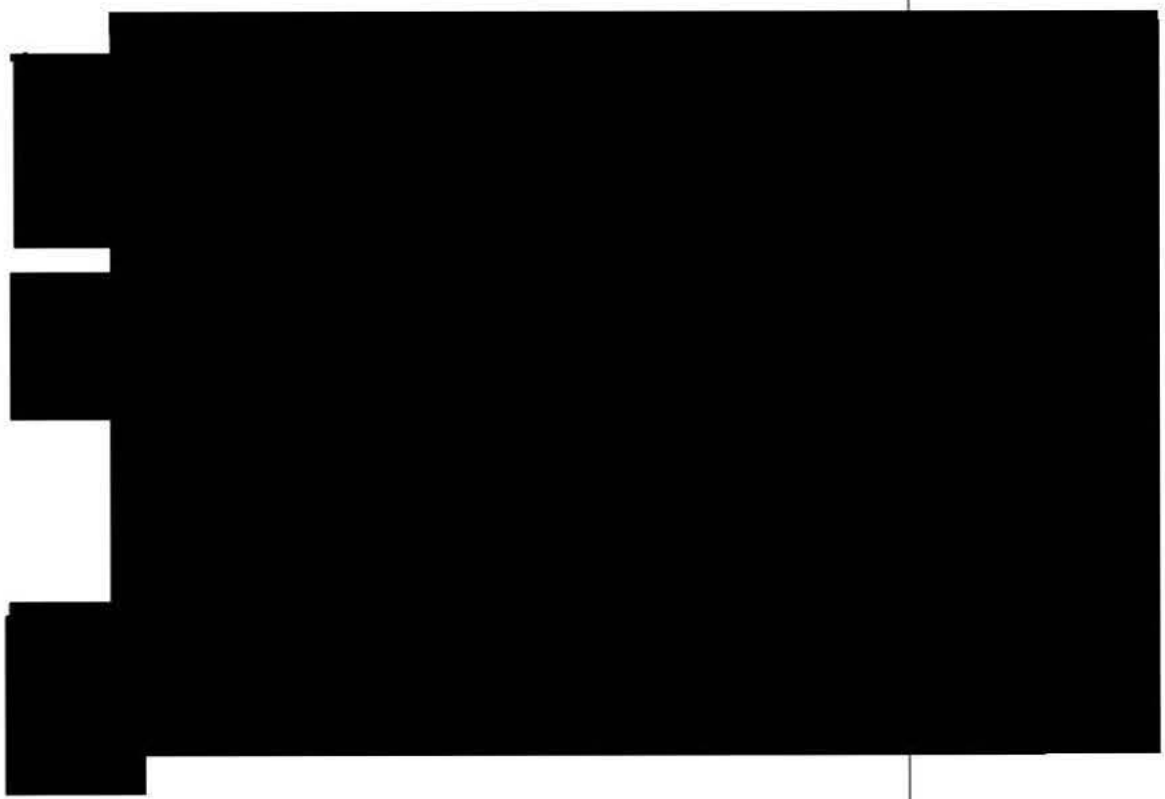
We are happy to provide the following responses to your questions:

Confidential Treatment Requested:

1. *Please provide more detail regarding your knowledge based authentication method. Specifically, what are the questions that will be asked; how many questions will*

IMPERIUM

be asked; how do you obtain the questions; what information do you need to collect from the parent in order to generate the questions?



The ChildGuard Service initiates the verification process for all parents and guardians by requiring them to provide Imperium with a name, address in the United States and age that Imperium can validate independently. The Service must then confirm that the verified address is the same as the child's and the verified age is at least 16 years older than that of the child.

After these initial verifications, the ChildGuard Service will attempt to verify the identity of the parent or guardian via the last four digits of their social security number. If the Service is unable to do so, it will then attempt to verify their identity by generating the KBA questions.

Confidential Treatment Requested:

2. *Please provide any analysis you have done of the efficacy of this solution (i.e., provide an analysis of how the method meets the standard laid out in the rule – that it is "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." This could include summaries of any testing done, public articles or studies regarding the efficacy of knowledge-based authentication, particularly as it relates to the questions you intend to ask; and any information or*

IMPERIUM

analysis you have done regarding whether children would be able to answer the questions you intend to ask. To the extent you base the efficacy of the method you intend to use on other knowledge-based authentication programs, please note whether you use the same questions and, if not, how they differ.

Imperium has a great deal of experience with dynamic KBA in connection with its other business services, which are widely used to prevent fraud in the market research industry. Imperium processes millions of records monthly and its clients consistently report a very high level of accuracy. In addition, Imperium uses KBA technology in conjunction with IP-based geographic location to correlate a user's self-reported physical address with the IP-based geographic address.

Many major companies that provide and/or require online identification verification solutions use dynamic KBA technologies, which remain a preferred advanced method for verifying identification. For example, LexisNexis Risk Solutions, Inc. recently acquired RSA Security, Inc.'s KBA technology. Credit bureaus, such as Experian (which markets its own KBA product), deal in the most sensitive personal financial information and use KBA technologies to verify user identification, including using the same or a similar set of questions as that proposed to be used initially in the ChildGuard Service.

The FTC has recognized KBA's role as a useful supplemental technology for online identification verification in the context of COPPA. In discussing "Verifiable Parental Consent" on the "Complying with COPPA: Frequently Asked Questions" page of the FTC's website, in Question 10 the FTC cites KBA as an example of the additional indicia of reliability that are available to verify parental consent in connection with apps.

A 2007 FTC seminar entitled "Security in Numbers: SSNS and ID Theft" included examples of the effectiveness of using KBA. One panelist, Jennifer Barrett, Global Privacy Officer at Acxiom Corporation, stated "behind the scenes in bringing the databases together that deliver these scores and this information, we use a variety of sources, both public and private, some of which contain SSN. Although we see a growing number of them not having SSN as time goes by. I would correlate the fact that multi-source confirmation in building these truth databases or these knowledge bases, for which we can do knowledge-based authentication, is as important as we have talked about multi-factor identification being important to the authentication process."

3. *Do you retain any information after a determination has been made? If so, what information?*

The only data retained is the result—i.e. whether the person passed or failed. Imperium retains none of the questions or answers.

IMPERIUM

Confidential Treatment

Per your email, Imperium wishes to request confidential treatment pursuant to 16 C.F.R. § 4.9(c) for the questions and responses under Questions 1 and 2 in the "Responses" section, which are labeled "Confidential Treatment Requested." The basis for that request is that those paragraphs contain trade secrets and confidential, sensitive commercial information for which there is a proprietary and highly competitive interest and, therefore, that information is not required to be made public pursuant to the exemption in 16 C.F.R. § 4.10(a)(2).

More specifically, the market for KBA anti-fraud solutions is very competitive and includes, as noted above, major companies such as LexisNexis and Experian. Specific technical information and methodologies concerning the ChildGuard Service is proprietary information for which participants in this market would have a highly competitive interest both in respect to the development and marketing of their own products and in order to "benchmark" the ChildGuard Service for competitive purposes.

Additionally, because the information for which Imperium has requested confidential treatment concerns technical information and methodologies used to produce the ChildGuard Service, rather than the functioning of the ChildGuard Service with respect to the end user (including the child, parent and potential fraudulent parties), maintaining the confidentiality of that information should not diminish the public's ability to assess the ChildGuard Service application for purposes of Section 312.12(a).

Imperium greatly appreciates the FTC's continued time and consideration with respect to this application. We remain available to respond to any additional questions or comments that you might have as the application process continues.

Sincerely,

Marshall C. Harrison
CEO, Imperium, LLC

CC:

Duane L. Berlin, Esq.
Lev & Berlin, P.C.
200 Connecticut Avenue, 5th Floor
Norwalk, Connecticut 06854