October 25, 2013

VIA OVERNIGHT MAIL

Donald S. Clark, Secretary
Federal Trade Commission
Room H-172
600 Pennsylvania Avenue, N.W.
Washington, D.C., 20580

Re: Application for Approval as a COPPA Verifiable Consent Mechanism

Dear Mr. Clark,

Please accept this letter as our formal request that the System identified below be approved as a mechanism to obtain verifiable parental consent in compliance with the Commission's Children's Online Privacy Protection Rule (the "Rule"), 16 CFR § 312 *et seq*. This request is made on behalf of iVeriFly, Inc. ("iVeriFly" or the "Company"). Based in Santa Ana, California, iVeriFly is dedicated to eradicating all forms of online fraud, and has developed a patent-pending technological solution designed to plug a significant gap in the security of online transactions.

Building on its core identity fraud prevention product, the Company has developed a unique COPPA-specific identity verification and consent solution (the "System") capable of providing an efficient, secure, and reliable method to obtain verifiable parental consent.

What follows is a brief description of the iVeriFly identity fraud product, followed by a description of the Company's COPPA solution, and an explanation of how its functions constitute newly available technology that provides a very high level of assurance that the person providing consent is, in fact, the child's parent, as contemplated by §312.5 (b)(1) of the Rule.

SECTION 1. THE IVERIFLY FRAUD PREVENTION TOOL

A. **Overview:** Nearly all Internet transactions, regardless of their purpose, require one party to provide the other with an email address, which then becomes the sole point of contact between them. This is the address to which receipts, confirmations, and other important communications will be sent. Until now, however, there existed no efficient, cost-effective method available to ensure that whoever someone is dealing with over the Internet is who they claim to be. Website operators have had no choice but to rely upon the accuracy of whatever email address their customer provided.

   This represents a fundamental flaw in Internet commerce that enables the unauthorized use of another person's credit accounts and other personal financial information. To make an unauthorized purchase, a criminal need only submit stolen credit card information and a fake email address to receive confirmation. The victim of the deception has no way of knowing that her identity has been compromised until the unauthorized charge appears on her credit card statement. The iVeriFly solution was developed to address this gaping hole in Internet security.

B. How it Works: Before a person can complete an online transaction (i.e., a purchase or website registration), iVeriFly sends an email to the address purportedly belonging to that person, which includes a link to the iVeriFly secure user interface. To verify their identity, the person must provide their name, address, and the last four digits of their social security number (SSN). iVeriFly then conducts an instantaneous search of aggregated non-FCRA consumer databases for that person's unique data record, and generates up to six random "out of wallet" multiple choice questions specific to that person.

Only the person identified as a party to the transaction will be able to answer the unique questions iVeriFly presents. All of them must all be answered correctly to verify that the person is who they claim to be. Establishing this fact also verifies ownership of their email address, and the iVeriFly subscriber can rest assured in the knowledge that any future communications will be sent to the right person. The next step in the process requires the person to enter their cellular number or landline. iVeriFly then sends a confirmatory phone call or text message to the number provided. Now the iVeriFly subscriber can be equally certain that their customer can be reached at that number. The entire process takes less than two minutes.

After a consumer goes through this process, any time that consumer attempts to make a purchase or engage in any other sensitive transaction with any iVeriFly subscriber, they will receive a randomly generated verification code via SMS or text-to-speech call, which they must enter into the appropriate space on the subscriber's website before the purchase or other transaction can be completed.

SECTION 2. THE IVERIFLY COPPA SYSTEM

iVeriFly's COPPA-specific solution incorporates the following steps:

1. A registration request that includes the parent's email address is submitted on an Operator's website;

2. The Operator sends the parent a verification email that details the Operator's privacy practices, and includes a link to the iVeriFly secure user interface.

3. The parent provides their name, address, and the last four digits of their SSN. The System locates the parent's unique data record[1], and generates up to six random questions drawn from the data record[2].

4. The parent must answer all questions correctly for a verification to be successful. After answering the questions correctly, the parent has confirmed that they are who they claim to be, and that their email address is genuine.

5. The parent is then required to provide their cellular number or landline.

[1] If the System is unable to locate a record, it will request the parent to provide their full SSN. If the full SSN does not locate a record, the System will display a "No Match" notice, and registration will be blocked.

[2] Sample questions presented by the System are attached as Exhibit "A," for which confidential treatment is requested.

6. The System then places a call to the parent, instructing them to do the following:

   (i) They must confirm that they are the parent of the child by pressing the "one" key on their telephone keypad.

   (ii) Upon receipt of an affirmative key press, the System asks the parent to confirm receipt of the Operator's notice of privacy practices by pressing the "two" key.

   (iii) Upon receipt of an affirmative key press, the System asks the parent to consent to their child's access to the Operator's site by pressing the "three" key.

   Failure to provide any one of the required key presses will block the registration.

7. After completing the process, the parent will be automatically directed back to the Operator's site to complete the registration. At the appropriate point in the registration process, the System will transmit the verification code, which the Parent must enter to complete registration.

8. The System will also produce and store a digital certificate for the Operator that confirms the affirmative key presses, and the date and time the verification occurred.

The System employs a similar process to obtain parental consent for Operators offering mobile apps targeted to children. Although they are not obligated to do so, Operators who want to offer parents oversight and control over their children's online activity may require a parent to enter the verification code every time their child attempts to log on.

SECTION 3. APPLICATION TO THE RULE

A. Distinction From Existing Methods: The iVeriFly consent mechanism represents newly available technology that provides a very high level of assurance that the person providing consent is, in fact, the child's parent, as contemplated by §312.5 (b)(1), and differs from the consent method enumerated in 16 CFR 312.5(b)(2)(v), which allows verifiable parental consent by "verifying a parent's identity by checking a form of government-issued identification against a database of information, where the parent's identification is deleted by the operator after such verification is complete."

Although the system does involve the cross-referencing of a form of government-issued identification (a partial SSN) against a database of information, this represents only a portion of the process, which further requires a parent to: (a) verify their identity by answering verification questions; (b) affirmatively confirm that they are the parent of the child, received proper notice, and consent to the registration; and (c) input a unique verification code at the appropriate point in a Provider's registration process. These additional steps distinguish the System's methodology from the method set forth in 16 CFR §312.5(b)(2)(v), and were developed to address the following faults inherent in that method:

1. **Reliability:** Simply cross-referencing a form of government identification against a database is an unreliable method for determining identity. Such a process only determines whether a person's name matches a number, and does nothing to ensure

that they are who they say they are. Requiring a person to answer questions drawn from an aggregated consumer database is necessary to make that determination.

2. **Affirmative Statement of Parentage:** Successfully verifying that a person is who they claim to be still does nothing to ensure that that person is the parent of a particular child. The System takes that into account by requiring the parent to confirm that they are the parent of the child seeking access, and further obtains confirmation that the parent has been provided with notice and consents to such access.

3. **Lack of Record:** An Operator that only cross references a form of identification against a database can only present a record of matching a name with a number. The iVeriFly System also retains a detailed record of the affirmation of parentage, receipt of notice, and consent to demonstrate proof of compliance.

Another aspect of the System renders it significantly distinct from any existing method referenced in the Rule: a parent who goes through the verifiable consent process with one subscribing Operator can provide consent to any other subscribing Operator without having to go through the process again.

When a parent first completes the verification process with Operator A, the System maintains a secure record of their verified email address and phone number. When the parent later attempts to register their child on Operator B's site, the iVeriFly system will recognize their email address and phone number as having been previously verified as belonging to that parent. Operator B can thus send the required notice to the parent's email address, obtain the parent's consent via key press, and transmit a verification code based on the previous verification, without requiring the parent to answer another set of verification questions.

B. Efficacy: The Company developed and tested the System to ensure it 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."

The Company first determined the number of questions to ask to obtain a reliable verification, and determined that the probability of someone guessing the correct answers to six out of six multiple choice questions with five answer choices is 0.0064%, or approximately one in 15,600. By way of comparison, according to the National Weather Service, the odds of someone being struck by lightning in their lifetime is one in 3,000. The Company therefore concluded the probability of a verification by guess to be statistically insignificant.

The second part of the process more directly addresses the Rule's reasonable calculation of parentage requirement. As previously stated, verifying identity via a dynamic knowledge-based authentication process, standing alone, does nothing to determine whether someone is the parent of a particular child. Therefore, the System requires an affirmative confirmation of parentage following verification of identity, thus satisfying the standard set forth in the Rule.

C. Subversion Analysis: In developing its COPPA solution, the Company also examined the likelihood of a child circumventing the System to gain access to an Operator's site without

parental consent. First, it should be noted that it is impossible for a child under the age of 13 to go through the process based on their own data record, as they are too young to have established one. A child may be able to secure the assistance of an unrelated adult to obtain the requisite consent, but the likelihood of someone falsely claiming that they are a child's parent solely to assist them in gaining unauthorized access to a website is sufficiently small as to be disregarded.

The Company also conducted several informal tests with children ranging between 10 and 12 years of age, to determine whether a highly precocious child could subvert the System in the absence of an adult conspirator. Although all of the children tested were able to provide their parent's name and address, none of them knew the last four digits of their parents' SSN. Acting under the assumption that a resourceful child would be able to obtain this information, the children in the test group were provided with the number, but were unable to successfully answer the verification questions drawn from their parent's record. Even if a child is able to obtain their parent's SSN and successfully answer the questions presented, they would still have to provide a phone number in order to falsely confirm their own parentage. The likelihood of any child overcoming every hurdle in the verification process is vanishingly small.

D. **Retention of Information:** Following the conclusion of the verification process, the System only retains the information that is reflected on the verification certificate: First name, last name, email address, phone number, and time/date stamp. This information is stored by the System and is only accessed to facilitate later verification requests. The Company does not maintain a record of the parent's SSN, or the questions they were required to answer.

The reliability of the iVeriFly System obviates the need to obtain a physical signature on a consent form to be returned via fax or postal mail, and enables Operators who do not charge for their service to obtain verifiable consent that is equally reliable to one obtained via a credit card. The System eliminates any need for a third party digital certificate, as one is issued whenever parental consent is verified. In addition, the reliability of the System, coupled with its ability to enable parents to monitor their child's access to approved websites, essentially eliminates the need for the additional confirmation required under the "email plus" method.

Based on the foregoing, we respectfully request the Commission approve our request to recognize the iVeriFly System as an effective mechanism to obtain verifiable parental consent in compliance with the Rule.

Yours truly,
iVeriFly, Inc.

Seth D. Heyman, Esq.
Senior Counsel

ATTACHMENT ONE

EXAMPLES OF VERIFICATION QUESTIONS

CONFIDENTIAL TREATMENT REQUESTED: Based on the sensitive nature of the method by which iVeriFly chooses the verification questions to be presented, we request that the answer to this question be treated as confidential and not subject to public review.

iVeriFly's standard COPPA package asks [redacted] multiple choice questions drawn from non-FCRA database categories, [redacted] These questions are referred to in the industry as "header" or "out of wallet" questions, in that they pertain to an individual's personal history, rather than their credit history. Thus, their answers can not be determined by a third party who has obtained unauthorized access to a credit report.

[redacted]