RelyID, LLC
12770 COIT ROAD, SUITE 1150
DALLAS, TEXAS 75251

June 30, 2010

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, C.D. 20580

Re: COPPA Rule Review, P014503

Dear Mr. Clark:

RelyID provides identity verification and authentication services to a variety of industries that want to ensure that they know who their customers are. We write in response to the Commission's request for public comment on the Commission's implementation of the Children's Online Privacy Protection Rule published at 16 C.F.R. part 312.

In particular, we want to address several questions the Commission asked about the portions of the Rule that address parental consent:

- 18c. Should any of the currently enumerated methods to obtain verifiable parental consent be removed from the Rule? If so, please explain which one(s) and why.
- 19a. Does the email plus mechanism remain a viable form of verifiable parental consent for operators' internal uses of information?
- 18b. Are there additional methods to obtain verifiable parental consent, based on current or emerging technological changes, that should be added to § 312.5 of the Rule?

We believe that the current methods do not fulfill Congress's objectives or parents' expectations and that the Commission should announce their prospective replacement with currently available technology that assures real parental consent.

1. Modifying Inadequate Methods to Obtain Verifiable Parental Consent

We believe that the Commission should significantly modify the methods that the Rule permits website operators to use in obtaining verifiable parental consent.

1.1 Removing Signed Consent Forms and Credit Card Transactions

Two current methods that the Rule specifies for obtaining verifiable parental consent do little ensure that the website operator has actually something that the average parent would consider to be verifiable parental consent. The main reason for this is that the children whom the Rule protects are far more sophisticated than any of the existing methods. *Spoofing verifiable parental consent is child's play under the Rule.*

The first current method to obtain verifiable parental consent is providing a consent form to be signed by the parent and returned by mail or fax. This method poses a barrier that is

trivial for children to circumvent. A child can simply print it off, sign it, and return it with a forged signature. Website operators have no way of knowing that the signature is one that the child forged by hand. Further, many homes now have printers, fax machines, and scanners that children use freely; they also have free access to sophisticated image editing tools. Particularly savvy children can scan a signature from some other document and place it on the consent form. This method simply does not obtain verifiable evidence of parental consent, nor does it assure that a parent has really consented to anything.

The second current method to obtain verifiable parental consent is requiring a parent to use a credit card in connection with a transaction. This method also poses a barrier that, while not trivial, is not all that significant. Our understanding (from asking our own payment processor) is that, when a website accepts a card for a payment, the website has no way of knowing whether the card is a "credit card" as the Rule requires as opposed to a check card or debit card. This is a problem for this method because more and more children have bank accounts for which the bank provides an ATM card that can be used as a check card. (And, even if the child does not, a friend may.) Second, many neighborhood grocery stores sell pre-paid Visa and Mastercard cards. Children can purchase these with little difficulty and no parental consent. Third, many website operators appear to believe that performing a card authorization, or charging a fee then refunding it immediately, satisfies this method, even if neither of these mechanisms cause an entry to appear on a card statement. Fourth, temporarily taking a credit card from mom's purse while she isn't looking is trivially easy in most households. With banks promoting online statements, parents are less likely to review their statements than when they came in the mail, so are less likely to catch the typical $1 fee to a website. Finally, the card networks themselves express doubt that card transactions verify age; Visa has previously asked the Commission to remove this method. This method simply does not obtain verifiable evidence of parental consent, nor does it assure that a parent has really consented to anything.

The presence of these first two methods suppresses the market for innovations that would otherwise emerge. The Rule's endorsement of these methods means that no website operator need do anything that prevents children from spoofing the Rule. Further, both of these methods give children a positive incentive to commit crimes such as forgery and credit card fraud, simply to get access to websites. Therefore, we believe that *the Commission should amend the Rule to expressly adopt a sunset date for these two methods.* The sunset date need not be imminent, but its existence will signal entrepreneurs to invest in superior methods.

1.2 Modifying Digital Certificates

The fourth method that the Rule specifies to obtain verifiable parental consent is using a digital certificate that uses public key technology. By itself, this is not a method of *obtaining* verifiable parental consent at all. As the Commission's staff heard at its recent roundtable, it is a method of *transmitting* a previously obtained verifiable parental consent. Therefore, we believe that *the Commission should amend the Rule to include the same qualification that applies to the fifth method: that the digital certificate provided after verifiable parental consent obtained through one of the verification methods listed in the Rule.*

1.3 Removing Email Plus

The email plus mechanism does not obtain verifiable parental consent at all. It simply does not ensure that a parent "authorizes" anything required by the COPPA statute. The main problem with this approach is that the child can create an email address to act as the supposed parent's email address, send the email from that address, and receive the confirmatory email at that address.

Like the consent form and credit card transaction, the availability of the email plus mechanism suppresses the market for alternative methods and encourages children to lie. Therefore, we believe that *the Commission should amend the Rule to expressly adopt a sunset date for the email plus mechanism*. We believe that this sunset date should be sufficiently after the sunset date for the consent form and credit card transaction methods for new methods to have gained widespread use.

2. Adding a Superior Method

There is at least one new method that we believe the Commission should add to the Rule. When an attorney decides whether to recommend a method that the Rule lists or one that the website believes to be superior, but that the Rule does not list, the attorney will be hard-pressed to recommend the innovative but unlisted method. In turn, a website operator is hard-pressed to justify anything that its attorney doesn't recommend. The Commission's endorsement of this method would encourage website operators to use a method that more reliably assures a parent's actual involvement.

2.1 What the Method Is

We believe that *the Commission should include the following method in the Rule*:

> the child's use of a username and password issued to an adult whose identity has been confirmed through one of:
>
> (a) a knowledge-based assessment that presents questions that children are unlikely to be able to answer (including through the child's use of information normally found in a parent's wallet);
>
> (b) a manual examination of copies of both privately issued documents to which children are unlikely to have access and governmentally issued identity documents;
>
> (c) an in-person examination of governmentally issued identity documents; or
>
> (d) other means of ascertaining identity of equivalent reliability.

2.2 How the Method Works

The concept behind this additional method is the emergence of reliable, purely online methods of proving identity. Large credit bureaus provide services that allow an adult with at least some credit history to prove who they are by answering questions online. Other providers appear to create similar questions through public records. The industry considers these questions to be "out-of-wallet" questions, meaning that someone who steals a wallet (including a child who raids mom's purse) will not be able to answer them. They certainly appear to be sufficient to prevent a child from correctly answering them without digging through the parent's financial records. While it is certainly possible that a child will do exactly that, it is far less likely than any of the problems we discuss above with methods that the Rule currently permits.

While these online methods of proving identity succeed in the overwhelming majority of the time (especially with people old enough to have children who are old enough to be online at all), there are instances in which they fail. When they do, identity authenticators fall back on a manual mechanism. Usually this is either an in-person review of governmentally issued ID or a remote review (e.g., by mail or fax) of both governmentally issued ID and other documents (like utility bills and bank statements) to which other people typically lack access.

These identity authentication services are in commercial use today, including in consumer reporting agencies and financial institutions, where high-reliability assurance of identity is critical. The innovation would be in using them for COPPA compliance. The only change needed would be that, once an identity authentication service confirms that the individual is an adult, either the website operator or the identity authentication service provides a username and password to the adult for the child's use on one or more websites. The child's subsequent use of that username and password on the site is evidence of the adult's prior consent. RelyID is prepared to make this service widely available, but believes that the long-term presence of the inferior methods discussed above may inhibit adoption of superior methods.

One may object to this method on the basis that it does not conclusively prove that the authenticated adult is the parent of the person who uses the username and password. But that hypothetical situation is pretty absurd: an adult goes online, provides his or her identity, and provides a username and password to someone who is not his or her child. None of the Rule's current methods prevents comparable problems. The fact that this method authenticates an adult at least gives the website operator reason to believe that the parent is actually involved; none of the other methods give any reason to believe this. Further, the fact that the authentication service knows the identity of the adult who received the username and password means that the hypothetical adult can be identified as a wrong-doer after the fact, which is much less likely with any of the Rule's other methods.

2.3 The Method's Advantages

This method has significant advantages over each of the main four main ways of obtaining verifiable parental consent:

- Compared to obtaining a signed consent form, the proposed method is far more certain to actually obtain consent from the parent, as opposed to forged consent from the child. The costs should be comparable between the two methods.
- Compared to performing a credit card transaction, the proposed method is also far more certain to actually obtain consent from the parent, as opposed to a charge to a card that the child holds or to the parent's card without the parent's knowledge. Initially, we expect the cost of the proposed method to be either comparable or slightly higher, but for the cost to drop rapidly with volume, because the vast majority of the cost is in initially authenticating the adult, with re-uses of that authentication having very low marginal cost.
- Compared to having the parent call the website operator, the proposed method is of comparable reliability on average, but is probably more consistent. That is, when someone calls the website operator, the website operator's personnel will simply make a mistake through human error, at least some of the time. The proposed method eliminates that source of human error for the adults whom it authenticates

automatically. We would anticipate that the cost would be lower than a phone call, simply due to the labor expense of having someone available to answer the phone 24 hours a day.

- Compared to the email plus mechanism, the proposed method actually obtains consent, which email plus does not. Further, it is much more likely to actually result in parents having control over their children's online activities. Of course, the ineffectiveness of the email plus mechanism makes it cheaper than the proposed method.

3. Resisting Methods that Lower the Standard

We would also like to comment on two other methods that we believe others will propose. We believe that both of these amount to a watering-down of already weak standards.

3.1 Identity Verification without Authentication

The first is a set of similar methods that involve a form of identity verification that does not rise to the level of identity authentication. Each of these methods involves the verification of an identifying number. Common examples are the last four digits of the social security number or the driver's license number. Companies can then check this information against certain data sources. This check does not confirm that the identifying number actually belongs to the individual at the computer; it just confirms that the number was issued to someone and may confirm the name of the person to whom it was issued. These methods have less reliability than carrying out a credit card transaction. They show that the person at the computer has access to a number on a card or document. Like a credit card, those cards may be in mom's purse; unlike a credit card, the verification will never show up on a bill that mom gets. We believe that *the Commission should not amend the Rule to adopt any method similar to these*; if it does so, then *the Commission should also amend the Rule to expressly adopt a sunset date for any method similar to these.*

However, the Commission may also want to consider adopting these identity verification methods in two scenarios. First, the Commission could require them as *supplements* to existing methods of verifiable parental consent. For example, a signed consent form *plus* a social security number verification is better than a signed consent form standing alone. Second, the Commission could require them as a *substitute* for the email plus mechanism. Confirming the last four digits of a social security number is better than sending an email to an address that a child can set up for himself or herself.

3.2 Electronic Signatures

The second possible proposal is the idea of substituting an electronic signature for a manual one on the consent form that a website operator may obtain. While we agree that an electronic signature ought ideally to be as good as a physical signature under laws like E-SIGN and UETA, neither of those statutes was written for a context in which forgery is the primary problem. The problem with the consent form method is that kids can forge their parent's signatures. Allowing an electronic signature greatly worsens that problem. Kids treat actions they take online as being less real in many ways than actions they take offline. Having to print off a document, forge a signature on it, and fax it back is much more intimidating than typing a parent's name and setting up a second email address. Therefore, we believe that *the Commission should decline to adopt an electronically signed consent form, by itself, as being verified parental consent*.

4. Summary

The technology exists for website operators to actually obtain real parental consent, as Congress intended and parents expect. The Rule permits children to avoid this requirement through trivial effort. Therefore, the Commission should modify the Rule to end, with fair warning to website operators, the methods that allow children to do so.

If the Commission has any questions about our observations, you can contact me at (866) 588-9288 or Laura Kendall (our Senior Vice President of Marketing and E-Commerce) at lkendall@relyid.com

Very truly yours,

RelyID, LLC

By: _____
Chris Lemens, its General Counsel