Date: 11/2/15
Riyo Verified Limited
c/o Davis & Gilbert LLP
1740 Broadway
New York, NY 10019

Miry Kim
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Riyo Verified Limited Application for Approval of a Verifiable Consent Method

Dear Ms. Kim:

On June 30, 2015 pursuant to Section 312.12(a) of the Children's Online Privacy Protection Rule (the "Rule"), Riyo Verified Limited (formerly jest8 Limited) trading as Riyo ("Riyo") formally requested approval of a verified parental consent ("VPC") mechanism not currently enumerated in the Rule. We are providing the following additional information in response queries about the mechanism.

Confidential Treatment Requested:

Riyo wishes to request confidential treatment pursuant to 16 C.F.R. § 4.9(c) for this document in its entirety. The basis for that request is that this document contains information implicating trade secrets and commercially sensitive proprietary information regarding the technology, confidential information that is not required to be made public pursuant to the exemption in 16 C.F.R. § 4.10(a)(2).

Specifically, this document explains the process for the two distinctly separate steps, that together form the VPC method. It highlights the technology that aids [redacted] the automated technological parts of the process [redacted].

1. Document verification
2. Face match

A data flow diagram has been included at Appendix 1 to provide further clarity over the method. The text has been highlighted yellow to indicate where there is technology used in the process

Part 1 – Document verification

The parent uses their phone's camera or a webcam to capture an image of their photo ID. For verifications completed on native mobile apps, the software automatically detects the document edges and captures an image of the document when it is presented at a perspective that facilitates full analysis and when the document is held still, to ensure that image that will be of adequate quality for initial analysis.

The software then rotates and accurately crops the image of the document to the frame so that it is ready for analysis. This image is encrypted at AES 256 standards to protect consumer privacy. It is then sent to the Jumio platform, which generates a transaction request and initiates algorithmic analysis of the ID.

The method uses a series of processes that combine computer vision technology, algorithms and image forensics verify the document for authenticity and legitimacy. The processes completed include:

- Algorithmic analysis for document manipulation using computer vision technology. In this process, the computer vision technology detects the edges of the identification, crops the image to those edges, detects text and rotates the image appropriately, and enables data capture for further analysis.
- MRZ (Machine Readable Zone) OCR (optical character recognition) detection to assess whether or not there is an MRZ code on a document and to extract the code for checks. The MRZ code is found on an MRP (Machine Readable Passport). It includes information about the identification document and the person it identifies including name, passport number, nationality, date of birth, sex, passport expiration date and personal identity number. There may also be country-dependent, supplementary information. These are presented in alpha-numeric characters and the filler character "<". OCR detection ensures that the characters printed on the identification are consistent with the identity.
- Check digit calculation in MRZ Zones. The data structure of the lower machine readable line provides for the inclusion of check digits. Calculations confirm that the identification numbers that pertain to the document correspond to validly issued identification numbers.
- Cross-referencing data encoded in the MRZ code for an accurate reflection in data points.
- Syntax checks in more than 125 languages.
- Syntax check substantiates both the authenticity of the identity and assesses the environment for the face match to prevent a bad actor presenting an image (trying to pass it off as a real person).
- Data driven fraud checks, wherein an algorithm designed to, search for and detect anomalies in the characteristics of the identification submitted, alters to fraud risk and causes the process to abort.
- Blacklist database check compares the document image captured to blacklist database of known fraudulent identification documents. [redacted].

As a stand-alone VPC mechanism, Part One would provide a high level of assurance, comparable to Knowledge-Based Questions. Part One could only be circumvented by the theft or misappropriation of an identity document. Uniquely for a VPC method, the proposed mechanism offers a multi-factor solution with Part Two – Face Match. This provides assurance that even a stolen or misappropriated identity document could not be used to obtain VPC because it requires the rightful document holder to be present.

Part Two - Face Match

The parent is directed to use the device camera to take a photo of his or her own face (often referred to as a "selfie"). This image [redacted] is compared to the face displayed on the photo identification used in Part One, validating that the person is the rightful document holder.

To provide further assurance that a live person is present when submitting a photo, FMVPI uses so-called "Liveness Detection." [redacted]

FMVPI face match match verifications are [redacted] with the use of [redacted] This technology aids [redacted] fast, effective decision making:

- The identity document and selfie [redacted].
- Credentials are [redacted].
- Credentials are [redacted]
- [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]

[redacted]

- The results are then automatically returned as per the data flow diagram at Appendix 1.
- Results are then parsed using algorithms with a decision rule applied (*i.e.*, VPC was or was not obtained).

By combining automated algorithmic technologies [redacted] FMVPI mitigates both potential weaknesses (accuracy of algorithms and human error), ensuring that it is effective [redacted]

The entire process outlined above is completed in within 270 (two hundred and seventy) seconds, 95% of the time. The service, [redacted] operation twenty for hours a day, seven days a week with multi-language customer support and compatibility with over 125 countries.

The first part of the process could stand alone as a single process and still provide a comparable level of assurance that a method such as knowledge based questions offers. The addition of this second step, face match to document, provides a higher level of assurance than other VPC methods because the rightful holder of the identity document must be present to complete the process.

CONCLUSION

We hope that the information provided here will be valuable as the Commission considers the Riyo application for a new verified parental consent mechanism. We remain open to discussion with the Commission regarding the points herein or any other questions it may have.

Kind regards,

……

Tom Strange
Director
Riyo Verified Limited

Appendix 1

Netverify Data Flow: