United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Federal Trade Commission
Office of the Secretary

November 18, 2015

Jest8 Limited (Trading As Riyo)
Care of Allison Fitzpatrick
Davis & Gilbert LLP
1740 Broadway
New York, NY 10019

Re: Jest8 Limited's (Trading As Riyo) Application for Approval of a Verifiable Parental Consent Method

Dear Ms. Fitzpatrick:

This letter is to inform you that the Federal Trade Commission ("FTC" or "Commission") has reviewed Jest8 Limited's (trading as Riyo) ("Riyo") application for approval of a proposed verifiable parental consent ("VPC") method under the Children's Online Privacy Protection Rule ("COPPA" or "the Rule"). The Commission has determined that the proposed VPC mechanism is "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." Accordingly, the FTC approves the proposed method.

Section 312.12(a) of the Rule allows parties to request Commission approval of VPC methods not currently enumerated in the Rule.[1] This provision seeks to encourage the development of new VPC methods that provide businesses more flexibility while ensuring parents are providing consent for their children. COPPA requires an applicant for Commission approval of a parental consent method to provide (1) a detailed description of the proposed parental consent method and (2) an analysis of how the method is reasonably calculated, in light of available technology, to ensure that the parent providing consent is the child's parent.[2] Under COPPA, the Commission considers for approval a proposed VPC method, which if approved, can be used by the applicant or any other party. The Commission does not approve one party's specific implementation of a VPC method or a proprietary system under the relevant provision of the Rule. Moreover, the Commission does not opine as to whether COPPA-related services that are not integral to the proposed VPC method satisfy the requirements of the Rule.

[1] 16 C.F.R. § 312.12(a).
[2] 16 C.F.R. § 312.12(a); 16 C.F.R. § 312.5(b).

Riyo submitted a proposed VPC method for approval on July 1, 2015. The Commission published the application in the Federal Register on August 7, 2015.[3] The public comment period closed on September 14, 2015.[4] The Commission received four comments regarding Riyo's application.[5]

The proposed method involves "Face Match to Verified Photo Identification" ("FMVPI"), which combines photo verification identification with facial recognition technology via web and mobile devices. The proposed method involves a two-step process. The first step of FMVPI includes photo identification verification. The parent captures the image of his or her photo identification (e.g. driver's license or passport) with a phone's camera or a webcam. The authenticity and legitimacy of the identification document is then verified using computer vision technology, algorithms, and image forensics to analyze the fonts, holograms, microprint, and other details coded in the document to ensure that the photo identification is an authentic government-issued identification.

The second step of FMVPI involves facial recognition technology. After the photo identification document is authenticated, the system prompts the parent to take a photo of his or her own face with a phone camera or webcam. The system detects facial movements to ensure this photo is of a live person, rather than a photo of a photo. The image of the parent's face is then compared to the face displayed on the photo identification. Photos that do not meet the required level of quality to complete the face match are rejected. After passing these checks, both images are then reviewed by live agents who are trained to verify whether the photo on the identification card matches the photo submitted by the parent. Once the parent is verified as the holder of the identification card, the consent process is completed, and the identification information submitted by the parent is promptly deleted, within five minutes.

The proposed method is very similar to an existing VPC method already in the Rule, which calls for verifying a parent's identity "by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete."[6] The proposed method does not involve checking the government-issued identification against databases of such information, but, as noted above, does involve verification of the identification document to ensure its authenticity. The proposed method is more rigorous than the existing approved method in that it involves the use of facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the system at that moment. Both methods involve prompt deletion of the identification information collected from the parent.

---

[3] 80 Fed. Reg. 47429 (Aug. 7, 2015), *available at* https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-proposed-3.
[4] 80 Fed. Reg. 53482 (Sept, 4, 2015), *available at* https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-proposed-4.
[5] The comments are available at https://www.ftc.gov/policy/public-comments/initiative-619.
[6] 16 C.F.R. § 312.5(b)(2)(v).

After careful consideration of the application and the public comments that were submitted in this matter, the Commission has determined that the proposed FMVPI method satisfies Section 312.5(b)(1) of the Rule. Specifically, evidence demonstrates that, like the other approved VPC methods, a method that involves verifying a government-issued identification and then matching the image on that identification with the captured face of a live person can be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent" as required by the Rule.

Facial recognition technology is now being used to verify identity in a number of settings. For instance, retailers, financial institutions, and technology companies use facial recognition technology for safety and security purposes.[7] While facial recognition technology is not perfect, in recent years, facial recognition technology has rapidly improved in performance, and now can surpass human performance under some conditions.[8] Moreover, the proposed method involves one-to-one verification – comparing one image with a second image – which can be very accurate, in comparison to matching one image with thousands or millions of other images.[9] Moreover, the proposed method also entails review of the two images by trained personnel. In short, identity verification via facial recognition technology can be reasonably reliable for purposes of determining whether an individual pictured in a government-issued identification is the same person in the second image.

We received four public comments on the proposed method. The Center for Digital Democracy's ("CDD") comment raises several concerns. First, CDD questions the efficacy of facial recognition technology as a VPC method on the basis that it has not proven to be accurate or reliable.[10] As noted above, however, facial recognition technology is being used today in a variety of settings that require a significant level of reliability and accuracy. We believe that this technology is sufficiently accurate to accomplish the type of one-to-one matching required in this setting, particularly given that this matching is also reviewed by trained individuals. Our approval of this method rests on the one-to-one matching; we do not opine on any facial recognition method that involves checking a single photo against a database of many photos.

---

[7] *See, e.g.*, U.S. Government Accountability Office, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, July 2015 ("GAO Report"), at 8-9. For example, the Orlando International Airport has added facial recognition to its automated passport kiosks, which compare the traveler's face with the biometric information in their e-passport. *See* https://orlando.interplex.net/blog/orlando-airport-first-to-add-facial-recognition/. *See also* Riyo VPC Application, Appendix 1 (indicating that the Jumio facial recognition technology is being used by financial institutions, airlines, and other companies).

[8] *See* GAO Report, at p. 5, *citing* Alice J. O'Toole, P. Jonathon Phillips, Fang Jiang, Janet Ayyad, Nils Penard, and Herve Abdi, *Face Recognition Algorithms Surpass Humans Matching Faces over Changes in Illumination*, IEEE: Transactions on Pattern Analysis and Machine Intelligence, 29(9), 1642-1646 (September 2007), accessed April 24, 2015, http://www.utdallas.edu/~herve/Abdi-opjapa2007.pdf. *See also* National Institute of Standards and Technology, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009 (Gaithersburg, Md.: May 26, 2014).

[9] *See, e.g.*, http://jain.egr.msu.edu/face-recognition/ (indicating accuracy rate of up to 99%).

[10] *See* CDD's Comments at p. 3, *citing* Patrick Grother & Mei Ngan, *Face Recognition Vendor Test, Performance of Face Identification Algorithms*, May 2014. We note that this test focused on one-to-many, and not one-to-one, applications of facial recognition technology.

Second, CDD argues that children can easily circumvent the system because the FMVPI system authenticates the identity of the holder, not the parent-child relationship.[11] However, the Commission addressed this concern in the 2013 Statement of Basis and Purpose for the Rule in deciding to include government-issued IDs as an enumerated VPC method.[12] CDD also notes that children may have government-issued documents, such as passports, at an early age, raising the possibility that the facial recognition process could simply be authenticating a child. The software at issue, however, is able to perform an automated check of the individual's birth date and thus block efforts by underage users who possess their own valid documents to authenticate.

Third, CDD comments that Riyo's particular implementation of the proposed method poses a risk to consumer data because Jumio, the company that provides the facial recognition software that Riyo will use in implementing FMVPI, has a privacy policy that indicates that it will collect extensive data about its users, use the image for data extraction, and share the data with third parties.[13] Jumio's privacy policy indicates, however, that it "collects, uses, and discloses individual users' information *only* as directed" by the operator. (Emphasis in original.) In order to use this method, companies must follow the conditions set forth herein. Riyo's application makes clear that information collected will be promptly destroyed and that the information will not be used for any other purpose. Approval of the proposed method is conditioned on adherence to these conditions.

Three other commenters raise concerns about elements of the proposal. Two, in addition to CDD, state that the proposed VPC method should be rejected because it collects sensitive personal information from photo identification cards.[14] As noted above, one of the VPC methods enumerated in the Rule involves collection of government-issued identification information on the condition that the information collected is "promptly deleted."[15] In approving that method, the Commission recognized the sensitivity of the information, but concluded that "on balance, government-issued ID provides a reliable and simple means of verifying that the person providing consent is likely to be the parent, and … the requirement that operators delete such data immediately upon verification substantially minimizes the privacy risk associated with that collection."[16] The proposed method here requires that the information collected must be promptly deleted, within five minutes of collection, and thus is consistent with the existing exception for collection of government-issued identification.[17]

Another commenter recommends against approval because the proposed method does not verify that the parent has actually seen and consented to their child's data being collected and shared, and that an opt-out of data collection should be in place.[18] This is true of other VPC methods already approved under the Rule. In any event, operators who use this or another method to obtain verifiable parental consent must still comply with all other provisions of

[11] *See* CDD's Comments at p. 7.
[12] 78 FRN 3987.
[13] *See* CDD's Comments at p.8.
[14] *See* Comments of Kris Alman and Rebecca McCullough.
[15] 16 C.F.R. § 312.5(b)(2)(v).
[16] 78 Fed. Reg. 3972, 3987 (January 17, 2013), *available at* https://www.ftc.gov/policy/federal-register-notices/childrens-online-privacy-protection-rule-final-rule-amendments.
[17] 16 C.F.R. § 312.5(b)(2)(v).
[18] *See* Comments of Cheri Kiesecker.

COPPA, including those that require that operators provide a valid notice prior to collecting personal information and enable parents to exercise their rights to review or delete information collected from their children.[19]

Therefore, the Commission approves the use of facial recognition technology as a VPC method under COPPA, provided it is appropriately implemented as set forth above.

By direction of the Commission.

Donald S. Clark
Secretary

[19] 16 C.F.R. § 312.4; 16 C.F.R. § 312.6.