Date: 10/15/15
Riyo Verified Limited (formerly Jest8 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: <u>Riyo Verified Limited (formerly jest8 Limited) Application for Approval of a Verifiable Consent Method</u>

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. Riyo has since received questions pertaining to the mechanism and matters related to it. Those questions and matters are addressed herein.

Riyo wishes to request confidential treatment pursuant to 16 C.F.R. § 4.9(c) for those portions of the responses to sections 1, 2, 4 and 5 that are highlighted and labeled "Confidential Treatment Requested." The basis for that request is that the information contains trade secrets and commercially sensitive proprietary information. As this confidential information includes statistical data and information regarding technological processes, it is not required to be made public pursuant to the exemption in 16 C.F.R. § 4.10(a)(2).

1) Error-rates / accuracy when matching the camera captured photo with the identification

Jumio reviews error rates on a monthly basis based on its test dataset and to the extent possible, on verifications completed as a data processor on behalf of clients. The extent to which client data provides error rate analytics to Jumio is restricted by the client's preferences and privacy policies.

[redacted] Many Jumio clients operate in regulated industries. Moreover, they consider this commercially sensitive data [redacted]

[redacted]

The face match is scored as a percentage [redacted] It is improbable that an identity is both misappropriated and the person who misappropriates it is identical in appearance to its rightful holder; hence, [redacted]. Additionally, the FMVPI technology also includes [redacted]

By combining automated algorithmic technologies [redacted] ensuring that it is effective.

2) The means by which identification is authenticated

[redacted] government approved identity documents of over 125 countries, *i.e.*, passport, driver's license and at a more granular level (for each U.S. state).

Confidential Treatment Requested:

Checks and processes completed on the document include:

- Algorithmic analysis for document manipulation using computer vision technology;
- 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;
- Data driven fraud checks:
  - Check digit calculation in MRZ Zones,
  - Syntax checks, and
  - Value cross checks;
- Cross-referencing data encoded in the MRZ code [redacted];
- Syntax check substantiates [redacted] trying to pass it off as a real person);
- Blacklist database check compares the document image captured to blacklist database.

3) Privacy Policy

As detailed in the "Riyo CDD rebuttal," Riyo did not initially provide information related to its privacy policy because the review process focus is the VPC mechanism, not Riyo.

For context, Riyo has a license over Jumio technology. The license permits use of the technology in a number of different applications related to identity verification but not necessarily parents, children and COPPA compliance.

One of the license provisions allows Riyo to use, adapt, alter and maintain the Jumio technology on a globally exclusive basis, as required to satisfy COPPA compliance regulations and similar regulations or requirements in other territories worldwide. Jumio has not and does not plan to provide COPPA compliance services like VPC, and therefore its privacy policy is not directly applicable here.

The Jumio privacy policy relates to its own application and use of the technology outlined in the mechanism but is not indicative of the actual practices that would apply to parents using the VPC mechanism under the COPPA Rule.

Jumio is a data processor and not a data controller, and data captured by the technology is used for the purpose of the identity verification to meet the needs of the Data Controller (the Jumio client). The needs of the Data Controller vary depending on the industry.

In the case of FMVPI, data treatment specifics would depend on the mechanism operator, the company offering the online service to children and that company's policies. The sophisticated and effective technology in the FMVPI mechanism does make data capture easier but requires explicit consumer participation and consent. Actual data captured may be no different to a parent hand writing on a paper form for print-and-send consent, as opposed to computer vision algorithms being able to read their identity document to complete the form for them.

In the case of Riyo, we envisage safe harbor entities providing FMVPI to their COPPA compliant customers and [redacted]. We have also discussed Riyo obtaining COPPA compliance policies and safe seals for added assurance.

The CDD wrongly described practices around the VPC mechanism as "alarming" in a COPPA context because the Jumio privacy policy explicitly states that children age 13 or under should not use the technology and that children under 18 should not do so without parental consent. The method only proposes collection of parent data from parents and not children under 13.

4) Security and assurance over deletion in 300 seconds

The data retention period for PII obtained through FMVPI will depend on the technological capability of each specific FVMPI implementation / provider.

Riyo and Jumio policies dictate that sensitive data processed in the production environment, which includes PII, be retained for the minimum amount of time it is needed; based on operational needs (delivery of service) and legal and regulatory requirements that apply in the jurisdiction.

Data retained would be encrypted, [redacted]. However, once data has been deleted it is not possible to audit specific parental consents granted.

Riyo has set 300 second data retention period for data captured solely and specifically in connection with COPPA and VPC to minimize the risk to consumer information. This allows for the processing time (completed in 270 seconds 95% of the time) before data deletion. After that period of time, the data will be deleted from Riyo's systems.

Jumio uses commercially reasonable physical, electronic and procedural safeguards to protect personal information from loss or unauthorized access, use, modification, or deletion. Sensitive information is encrypted in transit and at rest to AES 256 (detailed later in this paper). Jumio is PCI DSS Level 1 compliant (as required for its payment-processing product but also applied to Net Verify, the technology that underpins FMVPI) and regularly conducts security audits, vulnerability scans and penetration tests to ensure compliance with security best practices and standards. These security practices are wholly applicable to Riyo and its use of the technology.

Confidential Treatment Requested:

[redacted]

5) Controls around sharing a parent's biometric data or PII with third parties

Parents maintain control over their biometric data and PII by providing consent to the use of their data and participation in the process. Third parties are referred to in the Jumio privacy policy but not in relation to the rights, obligations or access to consumer data, but to support the internal operations of the system.

[redacted] through which the system operates and data is processed.

Where Riyo provides FMVPI, the default will be to provide a client (the online operator) with confirmation as to whether or not verified parental consent was successfully obtained (*i.e*., the decision), as opposed to provision of the personally identifiable information on which it is based.

6) Explanation of how the mechanism is implemented, where described by Riyo as "Direct initiation with an operator structured to have linked child accounts."

In its submission to the Commission, Riyo proposed three different process initiations of FMVPI for VPC under the COPPA Rule. One implementation was described as follows:

> *iii Direct initiation with an operator structured to have linked child accounts*
>
> *This process would be the same as that presented for a CCM [Common Consent Mechanism] other than it would differ functionally because linked accounts created by a parent for their child would only be used for that specific operator's online service (i.e., it would not be used to verify and authenticate other products or used as a single-sign-on). This also differs functionally to collection of online contact information from a child because the operator owns or has licensed the FMVPI technology to provide the service directly to parents, as opposed to outsourcing the process to a third party compliance service provider.*

Explanation:

1. The parent registers for a verified account with the online service operator;
2. Parent completes verification process with an approved method (this could be FMVPI);
3. Parent creates an account for each child – linked to the parent ID / administrator account;
4. Child can use their account ID to access the product provided by that online service operator.

This is similar to a CCM because the parent has administration over their child's account but the child can have their own log-in credential for the service provider. The parent is still consenting to their child's participation prior to the collection of data from the child. Where it differs is the relationship that the parent and child have with an operator.[1]

How a business chooses to implement FMVPI will depend on factors such as size, maturity, internal policy, human and financial resources.

1) Smaller operators may want to integrate a CCM and Riyo may create partnerships with CCM service providers for them to integrate FMVPI.
2) A mid-size operator may want to maintain a direct relationship with users by interacting with Riyo instead of integrating a CCM. The operator may not want to develop its own security infrastructure to handle consumer data, so it may want Riyo to respond with a yes / no type response instead of receiving raw data to make a parental consent decision.
3) A large operator may want a closer relationship with users or have a higher level of know-your-client type requirements imposed on it by its legal team; such as the necessity for detailed audit trails in respect of verified parental consent. In this instance, the operator may interact with Riyo

[1] Although not related to COPPA, Facebook login offers a familiar and comparable example, acting as a CCM for other online services and allowing log-in to several services with only one online identity credential (the Facebook log-in information). The relationship with users is intermediated by Facebook. Here, the relationship would be intermediated by a CCM, and FMVPI would be the tool used by the CCM to give users the ability to provide parental consent across the CCM's partner services.

(or another FMVPI provider) but may want the raw data from the VPC process so that it can parse the data and apply its own decision-making logic to acceptance.

4) Lastly, an operator may not want to integrate a third party technology. A very large operator may decide to build its own FMVPI mechanism for VPC in connection with its portfolio of online assets and may create its own parent accounts with connected child accounts.

Examples 3 and 4 refer to Direct Initiation with an operator. The initial submission allows for a wide array of FVMPI implementations that would meet the reasonableness the Commission applies. Since the Commission approves the method not Riyo as a provider of it, Riyo did not limit the submission to its own operations and intended practices.

7) How are cipher suites and AES256 secure?

The general principal of encryption is the use of mathematically complex algorithms to encode data to prevent access and decoding by an unauthorized party that does not hold the encryption keys. The resistance of the encrypted (protected) data is impacted by the specific implementation and the complexity of the underlying cryptographic system.

A cipher suite is a set of cryptographic algorithms that specifies one algorithm for each part of the encryption process. AES ("Advanced Encryption Standards") is a symmetric block cipher created to meet the needs of the National Institute of Standards and Technology (NIST). It was subjected to analysis by the National Security Agency (NSA) prior to becoming a federal government standard and protecting classified information.

A block cipher is a method of encryption that uses algorithms and cryptographic keys. The term "block" refers to how they are applied to data. Block ciphers are applied to a block of data instead of each binary bit (a stream cipher).

There are three levels of AES: 128, 192 and 256. All encrypt and decrypt in blocks of 128 bits but differ in the length of the cryptographic key (denoted by the number). For example, AES 256 has a 256-bit key length. The 256-bit keys also have more rounds; rounds consist of processing steps including transposition, substitution and the input of the plain text being protected to create what is called "cipher text."

In lay terms this means that, even if Riyo or Jumio suffered an attack and data either in transit or at rest was accessed, it would could not be interpreted by the perpetrator. In the U.S., information classified as "Secret" may be encrypted to AES 128 and "Top Secret" information is encrypted to either AES 192 or 256. Riyo and Jumio use AES 256.

As a point of reference, email is rarely encrypted. Very few providers offer encryption and very few consumers implement encryption solutions available to them. This means that the data of a parent sending a consent form via electronic scan and email under "print and send" would be fully exposed; many consumer fax machines also do not offer encryption. FMVPI is far more secure.

Similarly, parent identity could be verified under the COPPA rule by checking government issued identification against a database of such information (to obtain VPC), the encryption protocols of these service providers are unknown and not prescribed, meaning that a parent's data could be at risk when in transit or rest. FMVPI reduces this risk by controlling the whole data cycle.

In summary, AES 256 is best practice and fit for protecting the information of parents and children.

CONCLUSION

We hope that the information provided here will be valuable as the Commission considers the Riyo application for a new parental consent mechanism. We remain open to discussion with the Commission regarding the points herein or any other questions it may have. If further detail is required in order to reach the decision of approval, we would welcome an all-parties phone call.

Kind regards,

………………………………

Tom Strange
Director
Riyo Verified Limited (formerly Jest8 Limited)