Date: 10/7/15
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: **Riyo Verified Limited (formerly jest8 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.

On September 14, 2015 during the public comment period, the Center for Digital Democracy ("CDD") submitted a request for the Commission to reject the VPC mechanism. It would appear from its comments that the CDD lacked certain information and knowledge to make a technological assessment. This response attempts to clarify some of the issues as well as inform the FTC as to where the CDD submission contained inaccurate or irrelevant information regarding the technology described in Riyo's application.

Riyo respectfully requests that the Commission gives due consideration to this rebuttal when assessing the VPC mechanism and reviewing the CDD comments. The inaccurate submission made by the CDD could have a significant impact on public perception and cause damage to Riyo as a business, and we wish to set the record straight.

REBUTTED COMMENTS

i. "Facial recognition technology is not reliable enough to protect children's online privacy"

CDD Statement:
First, the person uses their smartphone, webcam, or other camera to take a photo of a photo ID. Second, the person takes a photo of themselves. Third, the photos are sent to Jest8, which compares the photos and determines whether the person on the photo ID is the same person as in the second photo. If Jest8 determines the photos match, the consent process is complete.

Riyo response:
This statement fails to acknowledge "Section 1 Part One – Confirming the Integrity of the Photo Identification" in the Riyo submission. A parent can only complete the Face Match process after their photo identification has been confirmed as bona fide, not manipulated or doctored and is legitimate I.D. Face Match is the component of the mechanism that prevents a child using their parent's identification but the overall mechanism is multi-factor (confirming the document and then matching it to an additional image).

The exact process completed to authenticate the document will be covered in a direct response to the Commission's question on this matter, and using an overview and the example provided in Appendix IV.

CDD Statement:
Facial recognition technology is not accurate or reliable enough to be deployed in the sensitive area of children's online privacy.

Riyo response:
The Riyo application presents a number of case studies that support the adoption of the technology, including in areas with arguably higher risk than VPC, such as commercial airlines, a high security, and high threat environment. The CDD asserts that the Net Verify case studies are irrelevant because they are not in the domain of child privacy, despite the Jumio technology being exactly that proposed by Riyo, the clear evidence of effectiveness, positive customer feedback and having achieved a higher level of assurance in other use cases than is required for a child to use an online service.

CDD Statement:
Children will easily circumvent the system.

Riyo response:
Children could not easily circumvent the system. Although it is possible that a child has his/her own identity document and not beyond reason that a child could access that document without parental consent, the CDD has failed to appreciate the capability of the technology. Riyo VPC technology enables the fields of a document to be parsed and a decision rule applied to the consent decision.

Parsing is a process that can take a credential or field, such as the date of birth, from the identity document and can check for correct syntax, then turn the credential into a data structure to which a decision rule can be applied. For example, the technology is capable of (example provided at appendix iii) setting a rule to reject documents that have dates of birth below an established threshold. These decision rules would be set by the vendor offering VPC, and the technology would simply follow the rule.

CDD Statement:
Relying exclusively on facial recognition algorithms will undermine that principle because facial recognition has not proven accurate or reliable enough to avoid mismatches or incorrect results.

Riyo response:
FMVPI is as reliable at mitigating the risk of the wrong person, or a child providing consent as all other enumerated methods. The assurance level is higher than most methods other than perhaps a video conference. Even knowledge-based questions cannot guarantee that a bad actor with sufficient information cannot pass through its process.

The reason Riyo can offer a higher level of assurance than other facial recognition algorithm based technologies is because [redacted] This is why results relating to the analysis of the identification and the image of the parents' face may take up to two hundred and seventy (270) seconds to be processed; [redacted] ecure environment complying with PCI-DSS (Payment Card Industry Data Security Standard) standards for the protection of personal and credit card data. Further information can be provided about the center and this process if required.

CDD Statement:
Facial recognition technology has proven inaccurate based on many factors. Facial recognition technology still routinely returns false positives and false negatives based on "environmental factors, the quality of the matching algorithm, the scope of the database, as well as image quality."

Riyo response:
As occurred throughout the CDD's comments, the source relied upon here is dated and taken out of the context of the original document. Here, a submission made to the Federal Trade Commission by EPIC (Electronic Privacy Information Center), in January of 2012 reads more fully as follows:

> In the past decade, the accuracy of both facial detection and facial recognition techniques has grown significantly, though both false positives and false negatives routinely occur depending on environmental factors, the quality of the matching algorithm, the scope of the database, as well as image quality. https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf The EPIC article based this assertion not on proprietary research but on an article written by David Goldman of CNN.

In his article entitled "In the future, can you remain anonymous?", David Goldman cites multiple references that present a counter view to that presented by the CDD, finding that facial recognition is accurate:

> Since 1993, the false positive rate for identifying faces has been halved every two years, reaching 0.003% by the end of last year, according to the National Institute of Standards and Technology, U.S. Department of Commerce.
>
> Though computers still have difficulty identifying faces in low light or poor photo quality, programs are now able to capture a profile of a face, build a 3D model of it, rotate the photo and identify the person the face belongs to.
> *See* http://money.cnn.com/2012/01/13/technology/face_recognition/

In view of advancements in technology since 2012, it is also reasonable to conclude that technology has changed and improved even since the 0.003% was quoted.

CDD Statement:
In the area of law enforcement, the FBI has said "[c]onversion, lighting, angle, [and] resolution" can lead to inaccurate decisions.

Riyo response:
We note that the sources cited by the CDD date from 2012 and 2013, and that the quoted text is misattributed to the FBI (Mr. Samuel Jenkins (now retired) was at the time Director for Privacy for the Defense Privacy and Civil Liberties office, not the FBI), and those sources are now out-of-date. In fact, more than a year ago the FBI announced the full operational capabilities of its facial recognition services, evidence that the technology is now trusted among law enforcement. *See* https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

A representative of the Department of Defense has since confirmed that use of the source in question was incorrect. The representative also expressed that [redacted] office deals with policy, not technology. (DoD email response provided at Appendix II).

CDD Statement:
In a recent review of several commercial facial recognition algorithms, NIST concluded that performance of algorithms varies substantially. In this review, NIST tested six facial recognition algorithms by attempting to match faces to particular photos. For matching faces in high quality photos, the error percentages ranged from 4.1% to 20.5%. For matching faces in lower-quality and webcam photos, which Jest8 will allow in its proposal, the error percentages range from 11.3% to 66.9%.

Riyo response:
Facial recognition (detection) is not the same as facial verification. The report referenced, which is a "Face Recognition Vendor Test," features an assessment of technology that is not comparable because it is used to check a face against a discrete dataset of facial images; in this instance tested with datasets containing 160,000 to 1,600,000 faces. The subject's face also may or may not be in the dataset of potential matches. This one-to-many comparison is vastly

different to the FMVPI comparison of one document to one face, and should not be considered with respect to a different technology. Indeed, the report specifically excluded such technology: *"Out of scope: Not within the scope of this report are: performance of live transactional systems like automated border control gates."*

CDD Statement:
Several recent incidents have illustrated that facial recognition algorithms are not ready to be used as a parental verification method. One example involved an algorithm inaccurately identifying a person based on his photo ID. A Massachusetts man had his license revoked because the state's algorithm, which was designed to identify fake IDs, thought his ID was fake. However, his ID was real, he simply looked like another driver.

Riyo response:
Again, this reference from 2011 is out-of-date and no longer relevant to a discussion of facial recognition technology. Furthermore, the anecdote references one person having their license revoked but ignores the rest of the article, including the following:

> "Massachusetts bought the system with a $1.5 million grant from the Department of Homeland Security. At least 34 states use such systems, which law enforcement officials say help prevent identity theft and ID fraud. Last year, Massachusetts State Police obtained 100 arrest warrants for fraudulent identity, and 1,860 licenses were revoked because of the software, according to the Globe."
> *See* http://www.popsci.com/gadgets/article/2011-07/anti-fraud-facial-recognition-system-generates-false-positives-revoking-wrong-persons-license

If the total number of licenses checked by the system was 1,860 and only one was incorrectly revoked, the error rate was 0.0538%. Given that the system was funded by the Department of Homeland Security and is operational across 34 states, it is reasonable to conclude that it has demonstrable efficacy.

CDD Statement:
Another example involves Microsoft, which recently released an app that was designed to guess a person's age based on faces in photos. Its algorithms were so inaccurate that they turned into an Internet meme.

Riyo response:
This is further anecdotal evidence that is irrelevant to the discussion about the FMVPI technology. The Microsoft algorithms were designed to make inferences about the age of a person, not the identity of the person. Even if we were to take this CDD reference seriously, that the algorithm assigning the wrong age does not necessarily mean that the entire algorithm was erroneous. In their most basic form, algorithms have a learning rule and a decision rule and optimize through recursive executions. The Microsoft algorithm learnt that certain facial characteristics were common to people of a certain age. It could therefore be a case that the algorithm was accurate when making an assessment of facial characteristics; rather the people

using the product did not look their biological age, or did not match to the facial characteristics that had be ascribed to their biological age by the algorithm. Moreover, this application of an algorithm is different to matching a data representation of the face on a government approved photo identification document to that captured by a camera in real time.

CDD Statement:
In the law enforcement context, the FBI uses facial recognition technology for tracking potential criminals that could return inaccurate results up to 20% of the time.
https://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf

Riyo response:
The report citing an error rate up to 20% was produced in October 2010, and should not be given weight in a current discussion on technology. Furthermore, it was not a statistic based on the measurement or testing of law enforcement systems used by the FBI or a representation from the bureau, but was a pre-build requirement and not a post-build outcome. As noted above, in the time that has passed, the FBI has built and implemented software using facial recognition. The document cited stated that a system could permit an error rate of 20%, and references the use of facial recognition software in conjunction with other data. It states that because human agents double-check results retrieved with the technology as part of the process, the FBI could accommodate up to 20% error rate from the technology - a fundamentally different approach and methodology from FMVPI.

This is another example of misrepresentation and use of an example that requires the search of a face against a database of images that vary in quality. Riyo matches one-to-one and the quality of images is controlled because government identification requires front-facing images. The VPC software rejects photos captured that do not meet the required level of quality to complete and Face Match, requiring another photo to be taken.

CDD Statement:
Jest8 does not address any of these issues, nor does it offer any solutions or allege its proposal has better match rates.

Riyo response:
Riyo did not address the issues raised by the CDD because none of them relate to the VPC mechanism presented to the Commission. Riyo does have solutions, such as [redacted] Further details will follow about this control process and error rates in direct response to the Commissions questions on those topics.

CDD Statement:
Without further evidence from Jest8, the FTC should not assume the proposed algorithm will be sufficient under COPPA to protect children

Riyo response:
It seems disproportionate that the CDD is requiring Riyo to demonstrate a higher level of mechanism efficacy than financial institutions and airlines have, in view of their respective regulations and the higher level of risks in those environments. That the CDD defines the entire VPC mechanism as an algorithm indicates its lacking of technological knowledge and does not capture the control processes in place, such as [redacted].

CDD Statement:
While some of the examples used in this section relate to matching a face in a photo to a database full of photos, they still apply to Jest8's proposal. It is quite likely that a person using the FMVPI system will take a photo of themselves that is low quality (which will depend on the quality of the phone camera or the webcam), taken hastily or in dark conditions, or there may be other problems with the photos that could lead to false positives or false negatives.

Riyo response:
We are not sure why it would be "quite likely" that photos will be taken in dark conditions, but this is largely irrelevant, because an unsuitable (*i.e.*, too dark or low resolution) image will not pass through the process successfully. Therefore, the possibility of false positives is quite unlikely.

Picture and lighting quality could impact the ability of a parent to complete the process because the software would reject the images taken / document scanned. These "false negatives" would not however result in circumvention or increased error because of these quality controls. The impact for the user, if any, would be a less satisfying process due to having to repeat it.

CDD Statement:
Jest8 further claims that several large institutions "have used FMVPI to verify identity for a number of years." However, this misleadingly implies that many industries have accepted the technology and have no hesitations about it. Jest8 does not disclose that some industries have been reluctant to implement facial recognition software. In a recent GAO report, the GAO indicated that facial recognition "technology [is] not in broad use by financial institutions because of concerns over its accuracy."

Riyo response:
Review of the GAO report shows that the reference to facial recognition use by financial institutions was made by a representative from the American Bankers Association, who was repeating sentiment from two banks while confirming the use of facial recognition technology by another major U.S. bank:

> The American Bankers Association representative said at least one major U.S. bank uses facial recognition technology to identify robbery suspects, but two other major banks stated the technology was not in broad use by financial institutions because of concerns over its accuracy. *See* http://www.gao.gov/assets/680/671764.pdf.

But there are numerous other instances substantiating the increased use of the technology in the financial services industry. Evidence of biometric adoption includes the following:

> HSBC and USAA have rolled out a feature allowing consumers to identify themselves with a selfie. Facial recognition technology analyzes the contours of the face and compares those angles to the original photo registered with the account. In USAA's implementation, the user has to blink, to prevent imposters trying to log in with someone else's photo.
> *See* http://www.americanbanker.com/news/bank-technology/authentication-advances-may-finally-kill-passwords-and-pins-1074298-1.html May 2015.
>
> Vincent Endres, chief of corporate development at Hoyos Labs, says his company has been "swamped with interest" from banks in his company's facial recognition technology, which it's been testing with "several of the top 10 banks in the world. Some are looking to use this to let internal employees to log on without a password, some are looking at ATM applications," he said. "Private client groups want to get rid of tokens."
> *See* MasterCard Trials Facial and Fingerprint Biometric Payments in Europe and U.S., Jane Khodos | August 18, 2015 | Industry News, Insights & Research, available at: http://newsroom.mastercard.com/news-briefs/mastercard-trials-facial-and-fingerprint-biometric-payments-in-europe-and-u-s/.

CDD Statement:
Further, Jest8's limited "case studies" show only Netverify's use in situations unrelated to children's privacy (e.g., casinos and Bitcoin retailers) and do not prove the proposal would adequately protect children's privacy.

Riyo response:
The situations presented in case studies are not relevant to the assessment of child privacy suitability. That assessment is a measure of whether or not the technology works and the Commission considers the approach reasonable. That the technology has been adopted by companies worldwide and the CDD could find not one criticism of the efficacy of the Jumio technology, which underpins the Riyo VPC mechanism, shows that the technology does work; corporations emphasize its effectiveness and consumers enjoy the convenience. The protection of child privacy is a matter of empowering parents to make decisions with a convenient technology, provided by operators that maintain COPPA compliant policies.

ii. "Children will effortlessly circumvent Jest8's system"

CDD Statement:
Jest8's system would verify the ID holder, but children themselves can get photo IDs that would presumably pass through Jest8's algorithm without problem. Children can get learner's permits and even driver's licenses in many states at age 14. Minors can get a U.S. passport at any age. Given that young children have photo IDs, it could be children themselves that use the system to grant "parental consent." Alternatively, the child could consult an older sibling, an older friend,

or essentially anyone with a photo ID to get "parental consent." So long as the person taking the photo is the same person as on the photo ID, the system would appear to be satisfied. This process would be nearly effortless for the child and could occur entirely without the child's real parents ever knowing.

Riyo response:
Children could not easily circumvent the system. As described earlier in this rebuttal, the proposed VPC mechanism enables the fields of a document to be parsed and a decision rule applied to the consent decision, which would prevent the scenarios asserted by the CDD.

CDD Statement:
…the application does not assert that the proposal would take measures to ensure the person in the photo ID and in the separate photo is the child's parent. While this system could likely never establish with 100% accuracy that the person consenting is the child's parent, Jest8's application does not indicate that it checks for certain information that could increase the likelihood of the parent-child relationship. For instance, the proposal does not indicate that its algorithm verifies the birth date on the photo ID to ensure the person is a proper parental age. An ID with a birth year of 2002 or later is extremely unlikely to be the child's parent because that person is thirteen or younger. It is also unlikely that a person under the age of eighteen is a parent, which means Jest8 could probably filter for any birth dates past 1997. Though, if Jest8's algorithm did verify birth date, it must delete that information promptly after collection to minimize risk to consumer data.

Riyo response:
As referenced earlier in this rebuttal the VPC mechanism and technology allow for the recommendations that the CDD considers would be reasonable means of assuring that the person providing consent is the child's parent.

The Riyo submission expressed that the mechanism was designed to mitigate the risk to consumer data. The technology is not constrained by the limitations that the CDD raises. Each implementation to mitigate risk requires the use of more consumer data. To that extent, the CDD is contradictory and Riyo would be led by the Commission as to whether or not the checks in relation birth date were a requirement of the method being approved. The use of an email (sent to a parent, having obtained the permitted online contact information) combined with a VPC method is an accepted mechanism for assuring that the person providing consent is the child's parent. This is the mechanism already used by Child Guard Online (Imperium), which is why it has been proposed by Riyo as one FMVPI implementation.

iii. "The method poses a risk to consumer data"

CDD Statement:
The proposed process is used for data extraction in other contexts [and] the "Netverify" privacy policy indicates Jumio, the company that uses this system in other contexts, collects extensive data about users.

Jest8's proposal is adapted from contexts where one of the primary purposes of the system is the collect and extract data about people. Thus, the FTC should be wary of claims that applicant will delete the collected data. One potential solution, as discussed in the COPPA Statement of Basis and Purpose, would be to limit collection of "identification information to only those segments of information needed to verify the data." If the system verifies photos, it could blur other data and only verify photos.

Riyo response:
The collection and extraction of data from an identity document is required in order to authenticate and validate a document in the verification process. Additionally, as the CDD itself suggests, additional checks such as those based on birth date, provide further assurance of parental consent. The system does not only verify photos; it uses all data available to authenticate a document (example provided at appendix i and iii).

CDD Statement:
The Netverify privacy policy describes practices that would be alarming in a COPPA context. The privacy policy discloses that Jumio may collect, through Netverify, "name, physical address, email address, telephone number, social security number, driver's license number, state or national ID card number, passport number, other ID card number, credit or debit card number, CVV, expiration date, and/or date of birth." Jumio may also collect "a visually scanned or photographed image of your face and/or your identification card, driver's license, passport, utility bill, bank account statement, insurance card, or credit/debit card." Jumio shares all data it collects with "Third Party Data Controllers," which include its clients and other third parties with which Jumio does business.

Riyo response:
The CDD has misrepresented the Jumio privacy policy and its implications for consumers. The policy reads as follows (the "Services" refer to Jumio Net Verify):

> *Jumio makes the Services available to third parties for integration into those third parties websites applications and online services. Jumio collects uses and discloses individual users information only as directed by these third parties and accordingly Jumio is a mere processor of user information with respect to the Services and not a controller. Further, some features of the Services may be disabled or altered by the data controller.*
>
> *In general Jumio uses the personal and non-personal information that we collect in connection with the Services as discussed in this section of the Policy. However Jumio uses such information only as directed by the Third Party data controller that integrates the Services into its website application or other online service.*
>
> *Children's Privacy*
> *The Services are not directed to children under the age of 13 and Jumio will never knowingly collect personal or other information from anyone it knows is under the age of 13. We recommend that persons over 13 but under 18 years of age ask their parents for*

> *permission before using the Services or sending any information about themselves to anyone over the Internet.*

Jumio is a data processor and not a data controller. Data captured by the technology is used for the purpose of the verification as required by the Data Controller (the Jumio client). In the case of Jumio, the needs of a Data Controller may vary depending on the industry (*e.g.*, flight check-in or access to financial services). The data obtained, maintained and transferred depends on the application and requirements of the VPC mechanism and Process Initiation.

Data treatment specifics would depend on the operator (the Riyo client offering services to children) and its policies. Riyo understands that this process specifically relates to a mechanism, not Riyo as an operator and its implementation. The sophisticated and effective technology in the VPC mechanism could make data capture easier but only if the consumer consents. This is no different to a consumer opting to provide personal information by filling out an online form by typing, as opposed to computer vision algorithms being able to read their name and complete the form for them. We envisage each safe harbor providing the technology to its COPPA compliant customers.

Jumio uses commercially reasonable physical electronic and procedural safeguards to protect personal information against loss or unauthorized access, use, modification, or deletion. Jumio encrypts sensitive information both in transit and at rest. Jumio is PCI Level 1 compliant and regularly conducts security audits, vulnerability scans and penetration tests to ensure compliance with security best practices and standards.

The CDD is wrong to describe 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 with consent. Parents are not within the scope of COPPA and the method only proposes collection of parent data from parents. This is therefore not relevant in the context of COPPA.

CDD Statement:
Jest8 has not provided any proof or verifiable plan, only mere promises, that it will delete its data. It further provides no proof or plan that it will not share the extensive amount of data it will collect through this system with third parties. These practices are unacceptable under COPPA and should preclude approval of this application.

Riyo response:
Riyo has not provided a verifiable plan pertaining to data treatment because its focus in the application is the mechanism of verifiable parental consent. Any operator, Riyo or otherwise, can only be substantiated through future operations and if relevant, third party audits such as those completed by Kids Safe Seal and PRIVO. [redacted]

CDD Statement:
Jest8 has little to no track record in privacy protection, including addressing the interests of children.

Last, applicants appear to have little experience with protecting anyone's privacy, much less children's privacy. Jest8 and Riyo are relatively new companies. They were incorporated in December 2013 and have few assets. Tom Strange, Director of Jest8, has a background as a chartered accountant. Mr. Strange's lack of qualifications calls into question his ability to properly protect children's privacy through his software.

Riyo response:
Although we see little relevance to the parental consent mechanism at issue in the application, we note that Tom Strange is an active contributor to COPPA privacy discussion and was quoted, along with the CDD in the letter declining the VPC method proposed by Age Cheq. As a Chartered Accountant (ACA) registered with the Institute of Chartered Accountants in England and Wales, Tom Strange is required to maintain practices in accordance with the highest ethical and technical standards. Tom Strange qualified as an ACA with Deloitte. His clients included businesses in financial services, telecoms, energy and other regulated sectors. One U.S. client maintained bio-technology with the highest level of security clearance required because it could be used to create chemical weapons. Clients included public corporations that are more extensively regulated than private companies. This role provided Tom Strange with access to market sensitive information and created a necessity to protect the interests of clients and consumers through the work that Deloitte completed. Tom Strange has never been subject to a disciplinary proceeding. Subsequent to Deloitte Tom Strange worked in Mergers, Acquisitions and Private equity as a lead advisor with access to all information relating to a transaction. He operates with the highest level of trust and integrity and will service the privacy interests of children and their parents effectively.

Tom Strange has assembled a team of Non-Executive Directors with sector expertise and a track record of security and risk management at the highest level of governments and Fortune 50 organizations. Riyo is arguably more effectively and holistically equipped than the CDD.

That Riyo has consulted organizations like PRIVO, Kids Safe Seal, Child Guard Online and even the CDD itself demonstrates that Riyo takes its commitment to child privacy seriously.

[redacted]

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.

Kind regards,

……………………………….

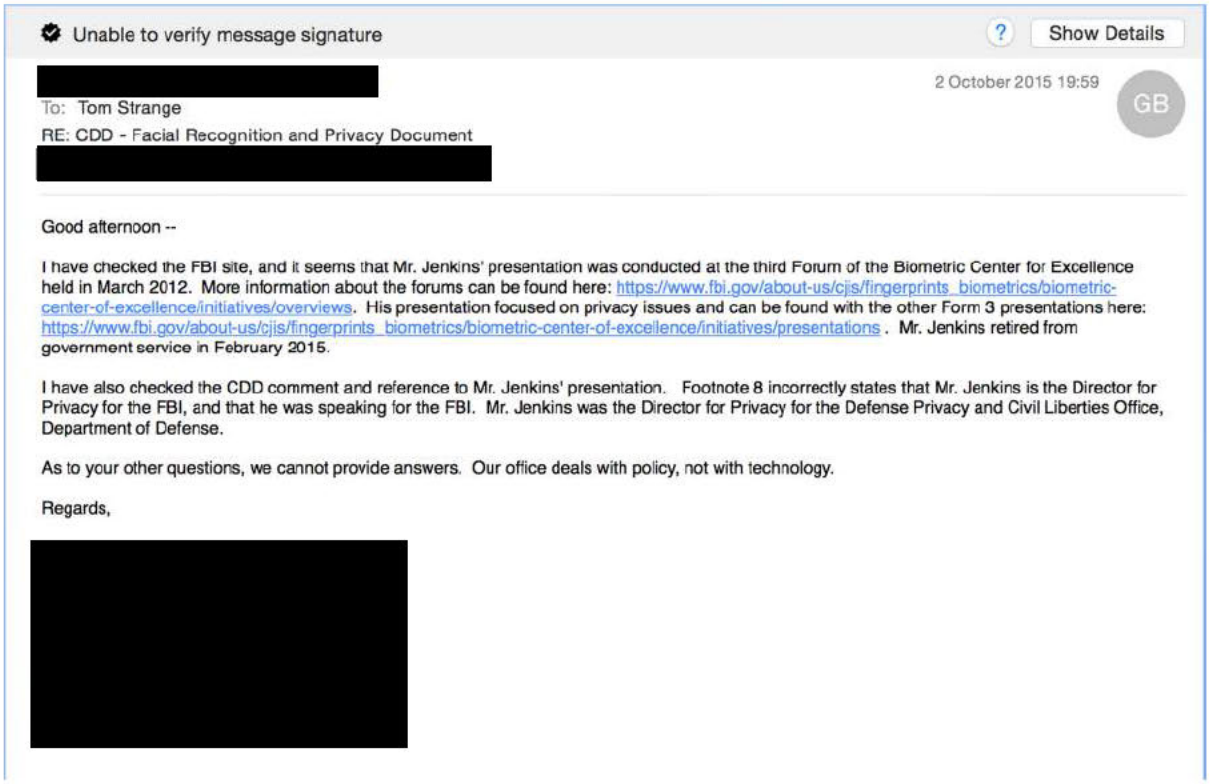
Tom Strange
Director
Riyo Verified Limited (formerly Jest8 Limited)

APPENDICES

I. Example data (based on U.K. Driver license) that enables parsing and additional controls.

[redacted]

II. U.S. Department of Defense Email Response



[redacted]

2 October 2015 19:59

To: Tom Strange

RE: CDD - Facial Recognition and Privacy Document

[redacted]

Good afternoon --

I have checked the FBI site, and it seems that Mr. Jenkins' presentation was conducted at the third Forum of the Biometric Center for Excellence held in March 2012. More information about the forums can be found here: https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/initiatives/overviews. His presentation focused on privacy issues and can be found with the other Form 3 presentations here: https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/initiatives/presentations . Mr. Jenkins retired from government service in February 2015.

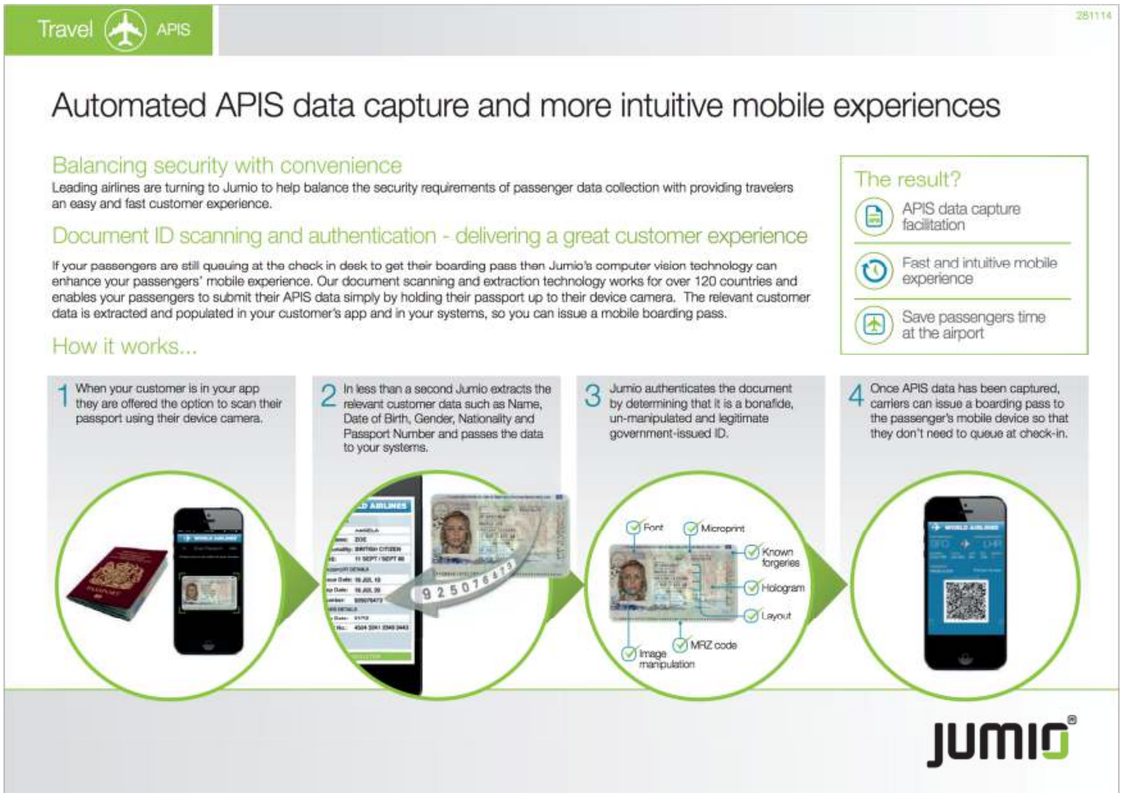
I have also checked the CDD comment and reference to Mr. Jenkins' presentation. Footnote 8 incorrectly states that Mr. Jenkins is the Director for Privacy for the FBI, and that he was speaking for the FBI. Mr. Jenkins was the Director for Privacy for the Defense Privacy and Civil Liberties Office, Department of Defense.

As to your other questions, we cannot provide answers. Our office deals with policy, not with technology.

Regards,

[redacted]

III. Jumio data capture and document authentication as implemented by airlines



Travel APIS

281114

Automated APIS data capture and more intuitive mobile experiences

Balancing security with convenience

Leading airlines are turning to Jumio to help balance the security requirements of passenger data collection with providing travelers an easy and fast customer experience.

Document ID scanning and authentication - delivering a great customer experience

If your passengers are still queuing at the check in desk to get their boarding pass then Jumio's computer vision technology can enhance your passengers' mobile experience. Our document scanning and extraction technology works for over 120 countries and enables your passengers to submit their APIS data simply by holding their passport up to their device camera. The relevant customer data is extracted and populated in your customer's app and in your systems, so you can issue a mobile boarding pass.

The result?

- APIS data capture facilitation
- Fast and intuitive mobile experience
- Save passengers time at the airport

How it works...

1 When your customer is in your app they are offered the option to scan their passport using their device camera.

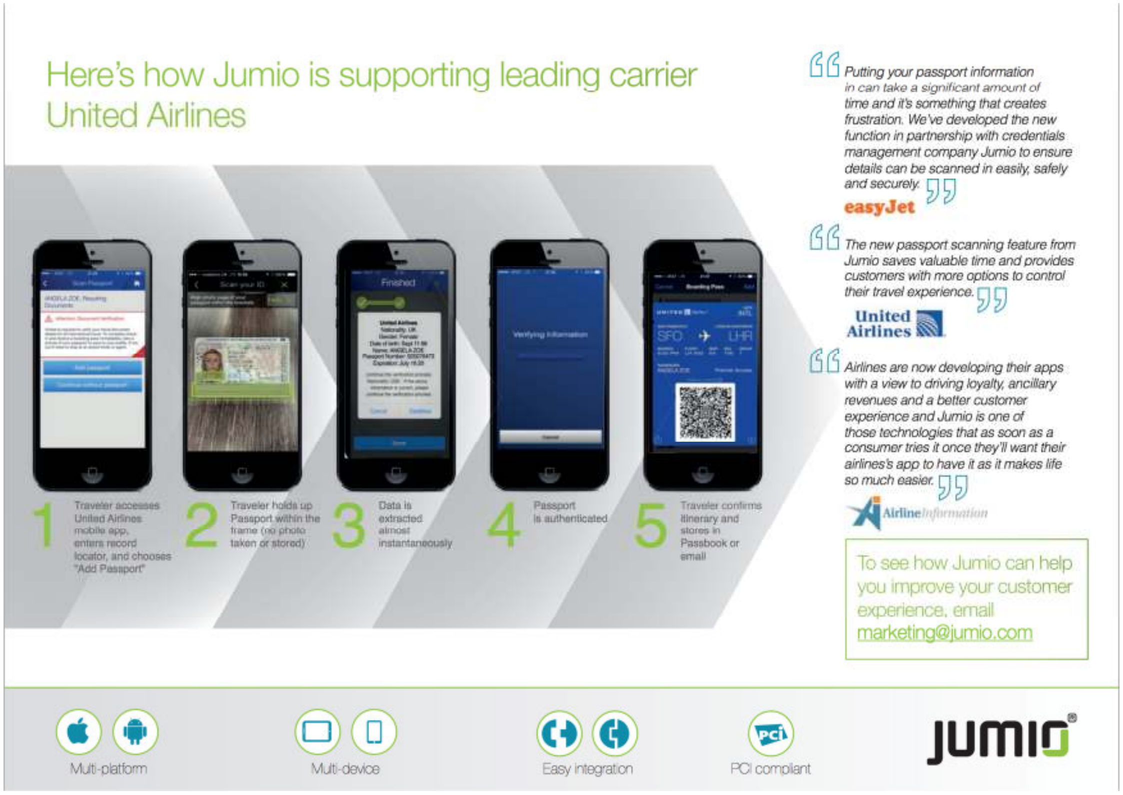
2 In less than a second Jumio extracts the relevant customer data such as Name, Date of Birth, Gender, Nationality and Passport Number and passes the data to your systems.

3 Jumio authenticates the document by determining that it is a bonafide, un-manipulated and legitimate government-issued ID.

4 Once APIS data has been captured, carriers can issue a boarding pass to the passenger's mobile device so that they don't need to queue at check-in.

JUMIO®

IV. Jumio airline implementation – consumer experience (showing data captured)



Here's how Jumio is supporting leading carrier United Airlines

1 Traveler accesses United Airlines mobile app, enters record locator, and chooses "Add Passport"

2 Traveler holds up Passport within the frame (no photo taken or stored)

3 Data is extracted almost instantaneously

4 Passport is authenticated

5 Traveler confirms itinerary and stores in Passbook or email

> *Putting your passport information in can take a significant amount of time and it's something that creates frustration. We've developed the new function in partnership with credentials management company Jumio to ensure details can be scanned in easily, safely and securely.*

easyJet

> *The new passport scanning feature from Jumio saves valuable time and provides customers with more options to control their travel experience.*

United Airlines

> *Airlines are now developing their apps with a view to driving loyalty, ancillary revenues and a better customer experience and Jumio is one of those technologies that as soon as a consumer tries it once they'll want their airlines's app to have it as it makes life so much easier.*

AirlineInformation

To see how Jumio can help you improve your customer experience, email marketing@jumio.com

Multi-platform

Multi-device

Easy integration

PCI compliant

JUMIO®