

FraudCheck.io

A database of customers marked fraud or suspicious by various Regulated Entities

Who is VideoCX.io (eka WorkApps)?

- 2017 incorporated Banking Tech startup
- India's most used Video KYC, Video Banking and Video PD platform
- 35 lac video customer sessions per month
- Used by 25 Banks, 40 NBFCs, and 10 Insurers
- Global ISV Partner with AWS

Top clients: ICICI Bank, Axis Bank, Kotak Bank, IDFC Bank, IndusInd, Yes Bank, DBS, JPMC, AU Bank, RBL, Suryoday, Ujjivan, Utkarsh, CSB, Shivalik, Utkarsh, Tata Capital, Poonawalla, Credit Saison, Piramal, Aditya Birla Capital, L&T Finance.

What is FraudCheck.io?

A central database of customers marked fraud, suspicious, criminal, terrorist or mule by Banks, NBFCs, Insurance companies and MFIs.

What data will be shared?

1. Regulated entity name
2. One-way Hashed value of customer name
3. One-way Hashed value of mobile number
4. One-way Hashed value of PAN number
5. One-way Hashed value of email ID
6. IP address
7. Live Lat Long
8. Customer address in text
9. Customer category – Suspicious / Fraud / Terrorist / Mule Account
10. VKYC system disposition and comments
11. Reason for marking fraud or suspicious (for ETB customers)
12. Any other notes
13. Date and time stamp of marking the case



When and how can a RE mark a Fraud?

During VKYC

(By VideoCX.io platform)

New status introduced in VideoCX.io platform called *Suspicious*.

It will have its own set of dispositions, which will be common across companies.

Once an Agent or Auditor marks it Suspicious, data will be shared with FraudCheck.io.

By any other onboarding journey

REs can mark a customer fraud or suspicions from any other onboarding journey and call an independent API service of FraudCheck.io to share the information.

Anytime after onboarding

REs can mark any ETB customer also fraud and share their data using an independent API service.

Bulk upload service will also be available for historic data sharing.

How can REs search in FraudCheck.io?

API request

RE can send either of the below fields of the customer they want to run the Fraud Check for in the API request

- Regulated entity ID
- Hash value of mobile number
- Hash value of PAN number
- Hash value of email ID
- IP address
- Lat Long
- Customer address

Any other customer data field can be added to the platform in a week's time.

API response (if match)

- Regulated entity name(s)
- Mobile number match (Yes / No)
- PAN number match (Yes / No)
- Email ID match (Yes / No)
- IP address match (Yes / No)
- Lat Long match (Yes / No)
- Email ID match (Yes / No)
- Customer address match (Yes / No)
- Fraud marking date
- VKYC Disposition
- Reason for marking fraud
- Customer category (Suspicious / Fraud etc)
- Notes

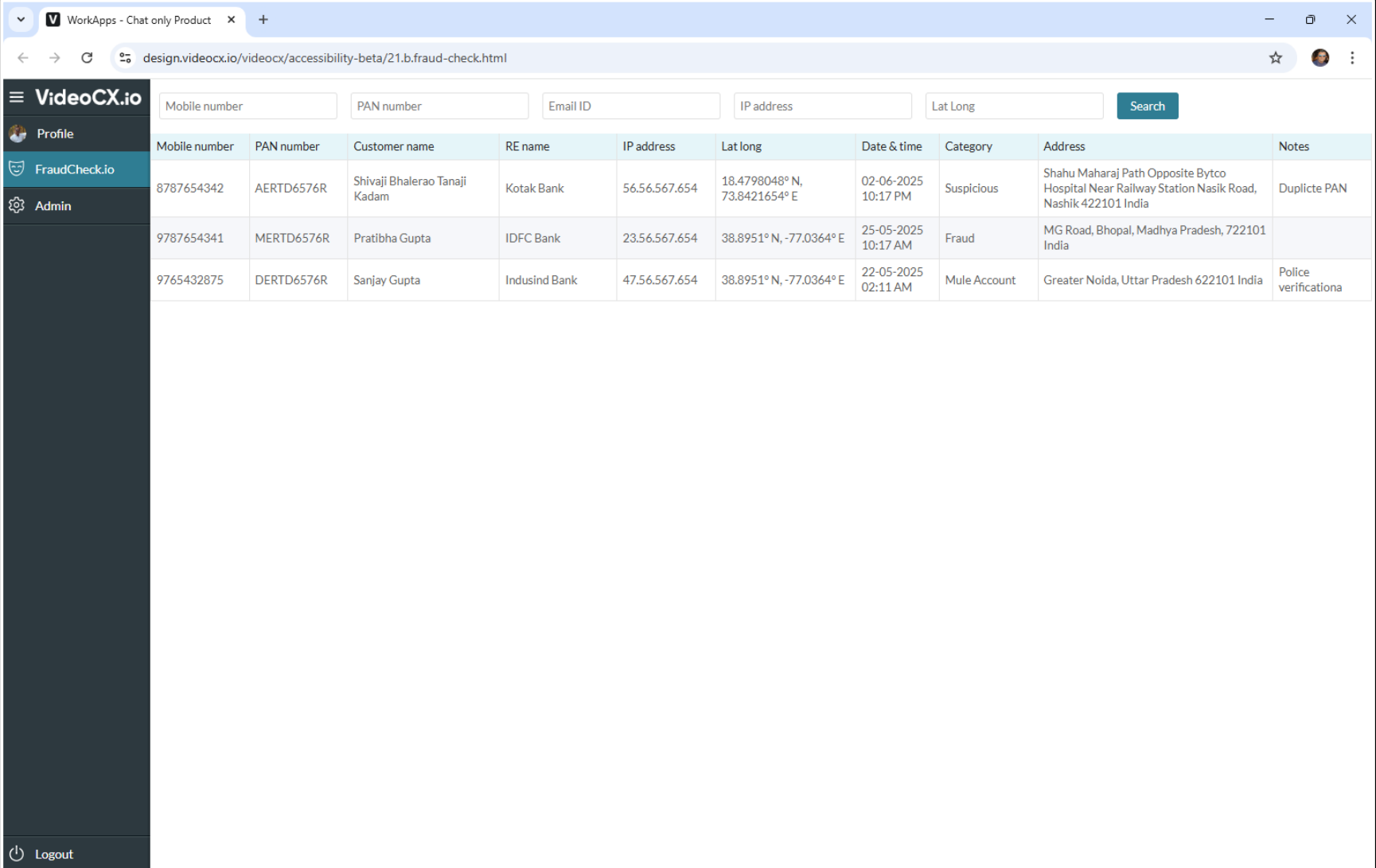
Data returned will be for all attempts made under that mobile, PAN, Email ID, IP address and Lat Long combinations, which could be from multiple REs.

Will there be a UI module also to search?

Yes

REs will have a UI module also to search using mobile number, PAN number, Email ID, IP address and Lat Long.

The module can be extended to bank branches and other internal teams.



The screenshot displays the VideoCX.io FraudCheck.io interface. At the top, there is a search bar with input fields for Mobile number, PAN number, Email ID, IP address, and Lat Long, followed by a Search button. Below the search bar is a table with the following columns: Mobile number, PAN number, Customer name, RE name, IP address, Lat long, Date & time, Category, Address, and Notes. The table contains three rows of data.

Mobile number	PAN number	Customer name	RE name	IP address	Lat long	Date & time	Category	Address	Notes
8787654342	AERTD6576R	Shivaji Bhalerao Tanaji Kadam	Kotak Bank	56.56.567.654	18.4798048° N, 73.8421654° E	02-06-2025 10:17 PM	Suspicious	Shahu Maharaj Path Opposite Bytco Hospital Near Railway Station Nasik Road, Nashik 422101 India	Duplicate PAN
9787654341	MERTD6576R	Pratibha Gupta	IDFC Bank	23.56.567.654	38.8951° N, -77.0364° E	25-05-2025 10:17 AM	Fraud	MG Road, Bhopal, Madhya Pradesh, 722101 India	
9765432875	DERTD6576R	Sanjay Gupta	Indusind Bank	47.56.567.654	38.8951° N, -77.0364° E	22-05-2025 02:11 AM	Mule Account	Greater Noida, Uttar Pradesh 622101 India	Police verification

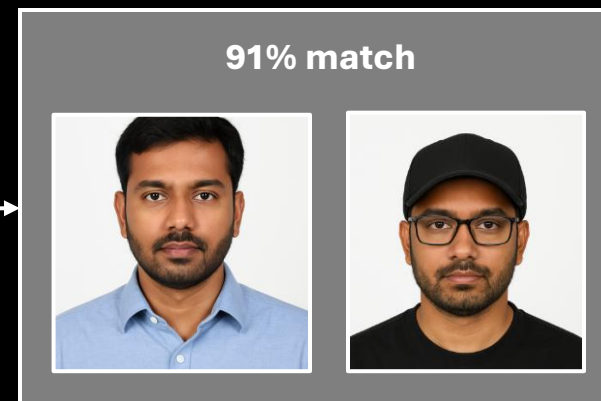
Using Face Match to find fraudsters



RE will send the customer's Aadhaar or Live photo in encrypted format to FraudCheck.io.



FraudCheck.io will create a vector of that and match it against all other photo vectors already present in the database.



FraduCheck.io database will return the face match % if positive and the RE name, disposition, customer category etc.

Identifying High Risk Locations

FraudCheck.io will maintain a central database of all High Risk Locations from across REs and make them available in API search against the customer's addresses or live location shared during Video KYC or any other type of onboarding.

Lat Long of customers who are marked fraud will also be stored in the same database and used while returning the Search API result.



Intelligent data matching

FraudCheck.io will do complete match and intelligent data matching for certain fields.

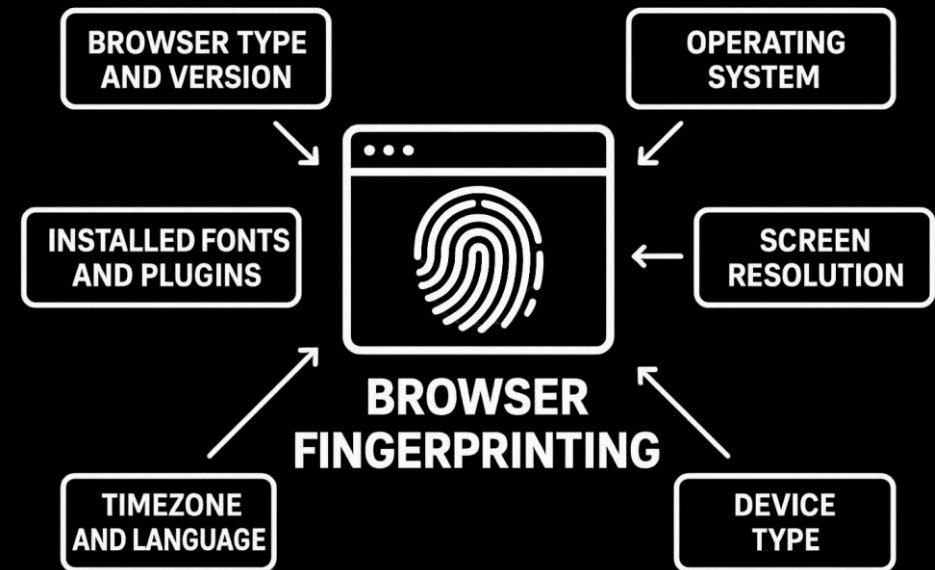
Email ID	If amarsingh1@gmail.com, amarsingh2@gmail.com, amarsingh3@gmail.com and amarsingh4@gmail.com are marked as fraud, then it will flag amarsingh5@gmail.com also.
Live Lat Long	Lat Long within X meters of other Lat Longs that are marked as fraud will be highlighted.
Customer address	Below addresses will be flagged as similar using <i>Entity Match</i> concepts 201, Crystal Bay, Kalyani Nagar, Pune, 411006 Crystal Bay, Kalyani Nagar, 201, Pune – 411006 Crystal Bay Apartments, 201, Kalyani Nagar, Pune – 411006

Finding fraudsters with Browser Fingerprinting

FraudCheck.io will create the logic for a unique browser fingerprint using popular JavaScript libraries like FingerprintJS.

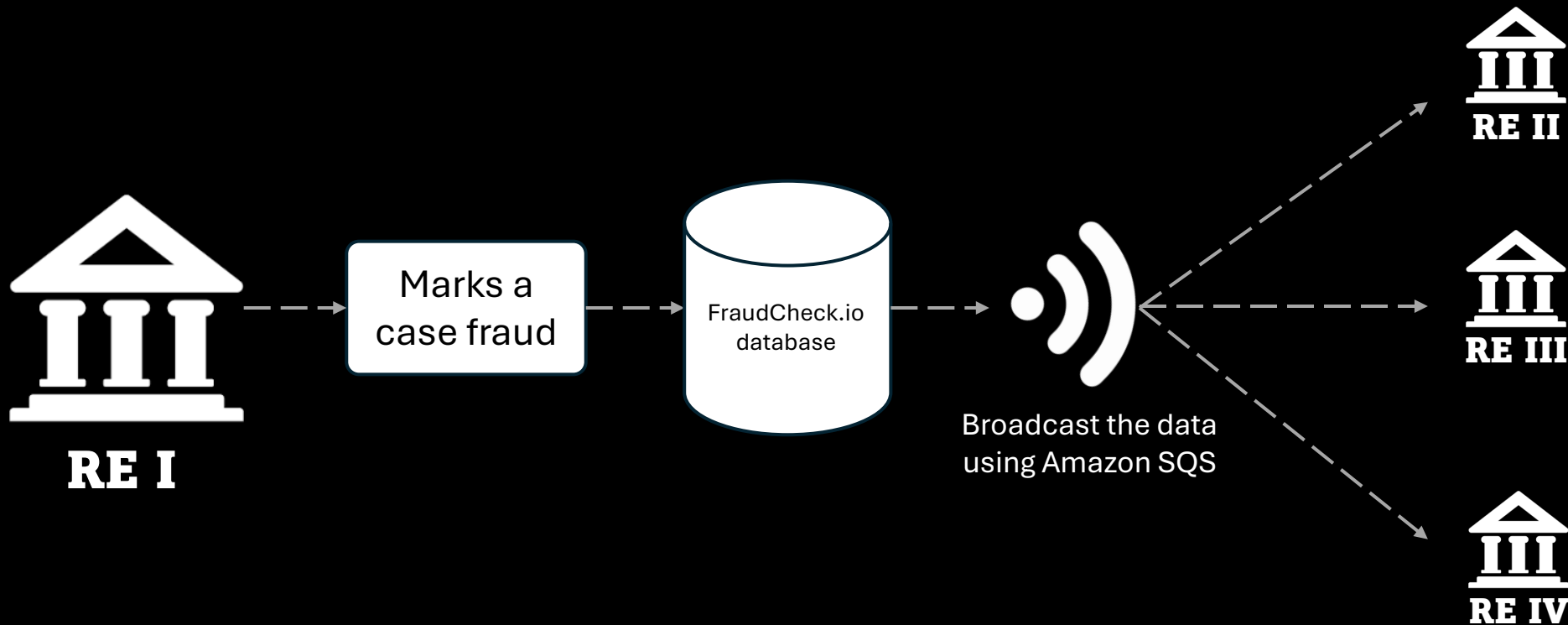
The browser data will be concatenated into a string and a Hash will be made from it.

The Hash will be used to compare attempts made from fraudsters.



Real time fraud alert and broadcast

FraudCheck.io will broadcast all cases that will be marked fraud or suspicious in real time using an Amazon SQS service, which REs can receive and block new or existing customers immediately.



What integrations are needed at RE end?

Add / Edit Data API

An API to add or edit data sent to FraudCheck.io from any other RE systems.

Same API will be used to remove the Fraud tag also.

Search API

An API to search data from FraudCheck.io database, which REs can integrate in their onboarding systems, CRM, Fraud systems etc.

Amazon SQS

A listener object at RE's end which will receive all real time alerts and broadcast sent by FraudCheck.io

** For REs using VideoCX.io VKYC system, the addition through VKYC will be a part of the VideoCX.io system itself.*

What will be the additional security?

- FraudCheck.io is hosted in AWS Mumbai region.
- API request will be authorized using a secret and key which will be unique for each RE.
- API request allowed from specific whitelisted IP addresses.
- API will also have payload level encryption.
- All other standard security measures will also be applied like Rate limiter, WAF, HTTPS.
- Periodic VAPT and Source code review reports will be submitted.



Who can add data to FraudCheck.io?

- Banks
- NBFCs
- MFIs
- Insurance companies
- Law enforcement agencies (Phase II)

What's our vision?

To be the outsourced fraud database management and detection team of Indian FSI companies.

Rudrajeet Desai
Founder, CEO and Product Head
+91-9730 669669
rudrajeet@VideoCX.io

VideoCX.io