KHOJ

PERSONAL DATA EXPOSURE DIAGNOSTICS

EXPOSURE REPORT

KHJ-SAMPLE-2026-MARKETING

Exposure Report

Personal data leakage analysis by Axiomaera.

✓ DPDPA 2023 ALIGNED

DATA PRINCIPAL

r*@gmail.com**

+91 98••••7547

Scanned · May 10, 2026 at 10:30 IST

ATI · 15-VECTOR COMPOSITE

CRITICAL

CLASSIFICATION

6	3	3	2
BREACHES FOUND	PLAINTEXT PASSWORDS	INDIAN SOURCES	PHONE HITS

"You are more exposed than 87% of Indians who have scanned with KHOJ."

— KHOJ ENGINE · CALIBRATED FOR THE INDIAN THREAT LANDSCAPE · 21 PARAMETERS · 15 VECTORS

SOURCES QUERIED

- HIBP · Breach Metadata
- Airavata · Email
- Airavata · Phone

Earliest exposure	2012
Latest exposure	2021
Data Classes Leaked	12 unique

ENGINE CALIBRATION

Calibration corpus	Indian breach corpus
Parameters	21 across 15 vectors
Threat bands	Low → Extreme
Indian risk markers	UPI · SIM-swap · Aadhaar
Issued By	Axiomaera Pvt. Ltd.

SHA-256 dfa896f3b1c216a4 a0d41f61b6b5533e da02c8dbf1d228eb 0de3beda428f32e3

POWERED BY AIRAVATA

PASSWORD HEALTH ANALYSIS

Every plaintext and hashed credential surfaced for this Data Principal, ordered weakest-first. Strength is assessed against length, character class composition, and known-bad pattern lists. Reasons cite the specific weakness driving each verdict — no opaque scoring.

TOTAL FOUND	PLAINTEXT	HASHED
4	3	1
across all breaches	readable as-is	offline-crackable

qwerty123	VERY WEAK	Adobe 2013
Rahul@123	WEAK	BigBasket 2020
linkedin2012!	OFFLINE CRACKABLE	LinkedIn 2012
5f4dcc3b…cf99 (MD5)	OFFLINE CRACKABLE	BigBasket 2020

INDIA-SPECIFIC RISK ALERTS

KHOJ surfaces three India-specific risk vectors absent from Western breach checkers — UPI fraud, SIM-swap, and Aadhaar-linked exposure. Alerts trigger only when the relevant data was actually leaked for this Data Principal; empty alerts are not displayed.

₹ UPI FRAUD RISK — HIGH

PHONE-LINKED PAYMENT APPS (GPAY, PHONEPE, PAYTM)

Your phone number appears in 3 Indian payments-adjacent breaches.

ACTION · Set a UPI PIN you never use elsewhere, and enable transaction alerts.

↻ SIM SWAP RISK — HIGH

TELECOM-DRIVEN OTP INTERCEPTION

Your phone + KYC adjacent details (name, address) are exposed.

ACTION · Call your telco and set a SIM-port PIN today. Don't share OTPs over phone.

i AADHAAR-LINKED RISK — MEDIUM

KYC CHAIN & UIDAI AUTHENTICATION

Identity fields (name + DOB + phone) sufficient to attempt mAadhaar lookups.

ACTION · Lock your Aadhaar biometric via UIDAI's portal until you next need it.

DATA EXPOSURE MATRIX

Rows are breaches; columns are data classes. Each dot is one verified exposure — clusters reveal the "jigsaw" identity an attacker can reassemble.

BREACH	CARD	DOB	EMAIL	GEO	GEOLO...	NAME	ORDER	PASSW...	PW	PHONE	USER
BigBasket · 2020		●	●			●			●	●	
LinkedIn · 2012			●						●		
DominosIndia · 2021			●		●	●	●			●	
Adobe · 2013			●					●	●		●
Canva · 2019			●	●		●			●		●
Juspay · 2020	●		●			●				●	

● Critical · passwords, financial
● Sensitive · phone, address, DOB
● Moderate · name, email, IP
Indian-origin breach

top columns shown

EXPOSURE FREQUENCY

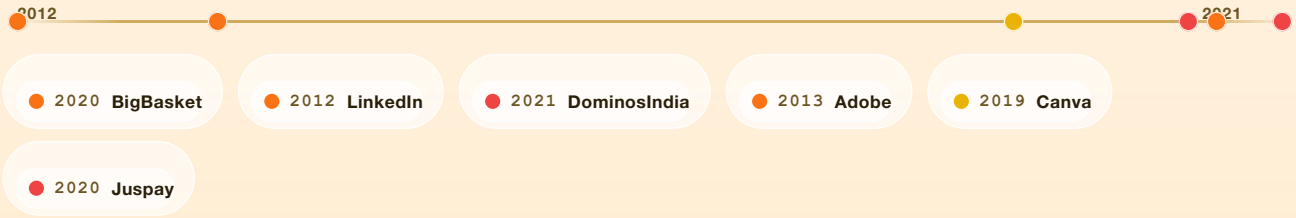
How many breaches surfaced each data class. Highest-frequency classes are easiest for attackers to corroborate across dumps.

Email addresses	6×	MODERATE
Names	4×	MODERATE
Passwords	4×	CRITICAL
Phone numbers	3×	SENSITIVE
Usernames	2×	MODERATE
Card hints	1×	MODERATE

+ 6 more data classes surfaced — full list on request

BREACH TIMELINE

Exposure window: **9 years** (2012 — 2021)



EARLIEST EXPOSURE	**LinkedIn · 2012** 14 years old	MOST RECENT EXPOSURE	**DominosIndia · 2021** 5 years old
INDIAN-ORIGIN SHARE	**3 of 6 breaches** 50%	YIELDED CREDENTIALS	**6 of 6 breaches** 100%

KEY DIAGNOSTIC METRICS

TEST	OBSERVED	REFERENCE	FLAG
Plaintext passwords Immediately usable by any actor holding the dump	3	0	▲▲ CRIT
Hashed passwords Recoverable via offline cracking	1	0	▲ HIGH
Phone-number references SIM-swap & UPI fraud vectors	3	0	▲▲ CRIT
Indian-origin breaches Domestic data fiduciaries breached	3	0	▲▲ CRIT
Compromised domains Distinct services holding leaked records	6	≤ 1	▲▲ CRIT
Exposure horizon Continuous years of active leakage	8 y	< 2	▲▲ CRIT

BREACH FORENSICS · EXPOSED CREDENTIALS

№ 01 **BigBasket** INDIA — HIGH

Breached October 30, 2020 · 2.0 crore records exposed · more than the population of Mumbai

Email addresses | Names | Phone numbers | Passwords | Dates of birth

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
PASSWORD	Rahu**123	AIRAVATA	PLAINTEXT · ROTATE NOW
USERNAME	rahul.sharma	AIRAVATA	*Identifier exposed*
PHONE	+91 98••••7547	AIRAVATA	UPI · SIM-SWAP
IP ADDRESS	103.21.244.0	AIRAVATA	*Geo / device hint*
NAME	Rahul Sharma	AIRAVATA	*Identity hint*
HASH	5f4dcc3b5aa765…	AIRAVATA	OFFLINE CRACKABLE
USERNAME	rahul.sharma	AIRAVATA	*Identifier exposed*

№ 02 LinkedIn

HIGH

Breached May 05, 2012 · 16.5 crore records exposed · more than the population of Mumbai

Email addresses | Passwords

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
PASSWORD	linked***012!	AIRAVATA	PLAINTEXT · ROTATE NOW
HASH	b89eaac7e61417…	AIRAVATA	OFFLINE CRACKABLE

№ 03 DominosIndia INDIA

CRITICAL

Breached April 18, 2021 · 1.8 crore records exposed · more than the population of Bengaluru

Email addresses | Phone numbers | Names | Physical addresses | Order histories | Geolocations

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
USERNAME	rahul.sharma	AIRAVATA	*Identifier exposed*
PHONE	+91 98••••7547	AIRAVATA	UPI · SIM-SWAP
NAME	Rahul Sharma	AIRAVATA	*Identity hint*

№ 04 Adobe

HIGH

Breached October 04, 2013 · 15.2 crore records exposed · more than the population of Mumbai

Email addresses | Password hints | Passwords | Usernames

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
PASSWORD	qwer**123	AIRAVATA	PLAINTEXT · ROTATE NOW

№ 05 Canva

MODERATE

Breached May 24, 2019 · 13.7 crore records exposed · more than the population of Mumbai

Email addresses | Geographic locations | Names | Passwords | Usernames

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
HASH	$2a$10$N9qo8uL…	AIRAVATA	OFFLINE CRACKABLE
USERNAME	rsharma	AIRAVATA	*Identifier exposed*

SHA-256 dfa896f3b1c216a4 a0d41f61b6b5533e da02c8dbf1d228eb 0de3beda428f32e3

POWERED BY AIRAVATA

№ 06 **Juspay** INDIA CRITICAL

Breached August 18, 2020 · 3.5 crore records exposed · more than the population of Mumbai

Email addresses | Phone numbers | Card hints | Names

EXPOSED CREDENTIALS & IDENTITY FIELDS

FIELD	EXPOSED VALUE	FOUND VIA	RISK
PHONE	+91 98••••7547	AIRAVATA	UPI · SIM-SWAP

DATA SOURCES & METHODOLOGY

All **breach metadata** — names, dates, record counts, data classes — is sourced from **Have I Been Pwned** (CC BY 4.0), the canonical public registry of confirmed data breaches. All **credential intelligence** is sourced through **Airavata**'s licensed breach intelligence integrations. These results are not available through free public breach checkers.

CLINICAL FINDINGS · KHOJ ENGINE ASSESSMENT

Subject's identity is present in **6 confirmed breach corpora** spanning a 8-year continuous exposure window. 3 of these are Indian-origin fiduciaries (UPI / telecom / e-commerce surface). **3 plaintext passwords** detected — readable by any actor in possession of the dump. Phone-number references in 3 dumps elevate SIM-swap and UPI-fraud risk above population baseline. Composite Khoj Threat Index resolves to **78 / 100 (CRITICAL)**, placing this holder more exposed than 87% of scanned Indians.

INDICATED ACTIONS · TIME-SLICED RESPONSE

№ 01	FIRST 24H	Change passwords on every site where you reused 'Rahul@123' or 'qwerty123'.
№ 02	FIRST 24H	Enable TOTP-based 2FA on Gmail, banking, and primary social accounts today.
№ 03	FIRST 24H	Set a SIM-swap PIN with your telecom provider (Airtel/Jio/Vi all support this).
№ 04	THIS WEEK	Remove your phone number from public profiles on LinkedIn and Facebook.
№ 05	THIS WEEK	Freeze your CIBIL credit file via the official portal — prevents fraudulent loans.
№ 06	THIS WEEK	Audit OAuth/SSO connections in Google/Apple ID and revoke anything unfamiliar.
№ 07	THIS MONTH	Switch to a password manager (Bitwarden, 1Password) for unique passwords.
№ 08	THIS MONTH	Enable transaction alerts on every bank account and UPI app.
№ 09	THIS MONTH	Review your Aadhaar authentication history monthly via UIDAI's mAadhaar app.

YOUR RIGHTS · DPDPA 2023

§ 12
Right to Correction and Erasure
Compel any data fiduciary to correct or delete your personal data. Email their Grievance Officer.

§ 11
Right to Access
Compel disclosure of what they hold about you and how it is processed.

§ 13
Right to Grievance
Escalate to the Data Protection Board of India, as and when constituted, after first approaching the data fiduciary's Grievance Officer.

COMPANIES ON THIS DOSSIER · Adobe · BigBasket · Canva · DominosIndia · Juspay · LinkedIn

IF THIS REPORT CAUSES YOU CONCERN

Data exposure is common and fixable. Follow the action items above. If you would like to talk to someone, these helplines are free, confidential, and operate around the clock.

Vandrevala Foundation
1860-2662-345
24/7 · Free · Mental health support

KIRAN Helpline
1800-599-0019
24/7 · Free · Government of India

— END OF EXPOSURE SCAN REPORT —