# Exposure Report

Personal data leakage analysis by Axiomaera.

✓ DPDPA 2023 ALIGNED

DATA PRINCIPAL

**r***@example.com**

+91 98••••3210

Scanned · October 23, 2026 at 10:30 IST

ATI · 15-VECTOR COMPOSITE




## CRITICAL

CLASSIFICATION

| 6 | 2 | 3 | 0 |
|---|---|---|---|
| BREACHES FOUND | PLAINTEXT PASSWORDS | INDIAN SOURCES | PHONE HITS |

*"You are more exposed than 73% of Indians who checked."*

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

## SOURCES QUERIED

- Breach Registry · Email
- Deep Search · Email
- Deep Search · Phone

| | |
|---|---|
| Earliest exposure | 2012 |
| Latest exposure | 2021 |
| Data Classes Leaked | 11 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. |



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED

*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

## 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 |
|---|---|---|
| 3 | 2 | 1 |
| across all breaches | readable as-is | offline-crackable |

| | | | |
|---|---|---|---|
| rah**1234 | WEAK | Grocery App 2020 |
| *dictionary word with trailing digits* | | |
| rah**1234 | WEAK | Job Network 2012 |
| *dictionary word with trailing digits* | | |
| 5f4dcc3b... (MD5) | OFFLINE CRACKABLE | Software Co 2013 |
| *MD5 hash · trivially crackable on consumer GPUs* | | |

⚠ **PASSWORD REUSE DETECTED**

`rah**1234` was found in **Grocery App, Job Network**. This password is compromised in 2 breaches. If used elsewhere, ALL those accounts are vulnerable.

## 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 UPI PAYMENT APPS**

Phone number leaked alongside Indian platform breach with credentials/financial data exposure.

**ACTION** · Check all linked UPI accounts for unauthorized transactions. Enable per-transaction SMS alerts. Set daily UPI limit to minimum needed.

### ↻ SIM SWAP RISK — HIGH

**TELECOM-DRIVEN OTP INTERCEPTION**

Phone number exposed 3 times across breaches.

**ACTION** · Call your operator immediately to add SIM swap protection. Port-out protection PIN if available.

### i AADHAAR-LINKED RISK — HIGH

**KYC CHAIN & UIDAI AUTHENTICATION**

Government IDs exposed, or DOB+address+phone combination enables identity reconstruction.

**ACTION** · Lock your Aadhaar biometrics at uidai.gov.in. Check Aadhaar authentication history for unauthorized usage.



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED

*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

## 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 | BANK | DOB | EMAIL | GOV ID | IP | NAME | PASSW... | PW | PHONE | ADDRESS | USER |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Grocery App** · 2020 | | ● | ● | | ● | ● | | ● | ● | ● | |
| **Job Network** · 2012 | | | ● | | | | | ● | | | |
| **Pizza Chain** · 2021 | | | ● | | | ● | | | ● | ● | |
| **Software Co** · 2013 | | | ● | | | | ● | ● | | | ● |
| **Payments Wallet** · 2021 | ● | | ● | ● | | | | | ● | | |
| **Design App** · 2019 | | | ● | | | ● | | | | | ● |

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

## 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** | 3× | MODERATE |
| **Passwords** | 3× | CRITICAL |
| **Phone numbers** | 3× | SENSITIVE |
| **Physical addresses** | 2× | SENSITIVE |
| **Usernames** | 2× | MODERATE |

*+ 5 more data classes surfaced — full list on request*

## BREACH TIMELINE

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




| | | | |
|---|---|---|---|
| EARLIEST EXPOSURE | **Job Network · 2012** 14 years old | MOST RECENT EXPOSURE | **Payments Wallet · 2021** 5 years old |
| INDIAN-ORIGIN SHARE | **3 of 6 breaches** 50% | YIELDED CREDENTIALS | **6 of 6 breaches** 100% |



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED
*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

## KEY DIAGNOSTIC METRICS

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

## BREACH FORENSICS · EXPOSED CREDENTIALS

№ 01 **Grocery App** INDIA — CRITICAL

Breached October 14, 2020 · 2.0 crore records exposed · more than the population of Mumbai

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

### EXPOSED CREDENTIALS & IDENTITY FIELDS

| FIELD | EXPOSED VALUE | FOUND VIA | RISK |
|---|---|---|---|
| PASSWORD | rahu**234 | VERIFIED | PLAINTEXT · ROTATE NOW |
| USERNAME | rahuls | VERIFIED | *Identifier exposed* |
| PHONE | 9876543210 | VERIFIED | UPI · SIM-SWAP |
| IP ADDRESS | 203.0.113.42 | VERIFIED | *Geo / device hint* |
| NAME | Rahul Sharma | VERIFIED | *Identity hint* |
| ADDRESS | Flat 4B, Example Residency, Pune | VERIFIED | PHYSICAL LOCATION |
| DATE OF BIRTH | 1994-08-12 | VERIFIED | IDENTITY VERIFICATION |



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED
*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

## № 02 Job Network

CRITICAL

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 | rahu**234 | VERIFIED | PLAINTEXT · ROTATE NOW |
| USERNAME | rahul.s | VERIFIED | *Identifier exposed* |

## № 03 Pizza Chain INDIA

SENSITIVE

Breached April 01, 2021 · 1.8 crore records exposed · more than the population of Bengaluru

Email addresses | Names | Phone numbers | Physical addresses

EXPOSED CREDENTIALS & IDENTITY FIELDS

| FIELD | EXPOSED VALUE | FOUND VIA | RISK |
|---|---|---|---|
| PHONE | 9876543210 | VERIFIED | UPI · SIM-SWAP |
| NAME | Rahul Sharma | VERIFIED | *Identity hint* |

## № 04 Software Co

CRITICAL

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 |
|---|---|---|---|
| HASH | 5f4dcc3b5aa765… | VERIFIED | OFFLINE CRACKABLE |
| USERNAME | rahulsharma92 | VERIFIED | *Identifier exposed* |

## № 05 Payments Wallet INDIA

CRITICAL

Breached March 29, 2021 · 1.1 crore records exposed · more than the population of Bengaluru

Email addresses | Phone numbers | Government issued IDs | Bank account numbers

EXPOSED CREDENTIALS & IDENTITY FIELDS

| FIELD | EXPOSED VALUE | FOUND VIA | RISK |
|---|---|---|---|
| PHONE | 9876543210 | VERIFIED | UPI · SIM-SWAP |
| NAME | Rahul Sharma | VERIFIED | *Identity hint* |



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED

*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

№ 06

## Design App

MODERATE

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

Email addresses | Names | Usernames

### EXPOSED CREDENTIALS & IDENTITY FIELDS

| FIELD | EXPOSED VALUE | FOUND VIA | RISK |
|---|---|---|---|
| USERNAME | rahul_designs | VERIFIED | *Identifier exposed* |
| NAME | Rahul S | VERIFIED | *Identity hint* |

### DATA SOURCES & METHODOLOGY

Every finding in this report comes from **confirmed, verified data breaches**. Credential-level results go beyond what free public breach checkers show.



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED

*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

## 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). **2 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 **67 / 100 (CRITICAL)**, placing this holder more exposed than 73% of scanned Indians.

## INDICATED ACTIONS · TIME-SLICED RESPONSE

| | | |
|---|---|---|
| № 01 | FIRST 24H | URGENT: 2 passwords are exposed, including 2 in plaintext. Change ALL passwords immediately, starting with banking and email. |
| № 02 | FIRST 24H | WARNING: The same password was found in Grocery App AND Job Network. This password is compromised everywhere you use it. Change it on ALL services. |
| № 03 | FIRST 24H | Your phone number is exposed 3 times. Contact your mobile operator TODAY to add SIM swap protection. Enable UPI transaction alerts. |
| № 04 | THIS WEEK | Check your bank statements and UPI transaction history for the last 90 days. |
| № 05 | THIS WEEK | Financial data exposed. Consider placing a credit freeze. Check your free credit report for unauthorised loans in your name. |
| № 06 | THIS WEEK | Enable two-factor authentication on EVERY account. Use authenticator apps (not SMS) where possible. |
| № 07 | THIS MONTH | Install a password manager and change EVERY password to a unique, generated one. |
| № 08 | THIS MONTH | File data erasure requests under DPDPA Section 12 with all breached companies. Template: 'I request complete erasure of my personal data under Section 12 of the Digital Personal Data Protection Act, 2023.' |

## 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** · Design App · Grocery App · Job Network · Payments Wallet · Pizza Chain · Software Co



© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED
*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*

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 —

**SHA-256** 1880dea4a6810e28 509a87fbfc09901e 33dc4b92426efa72 71d730ffd613b04a

POWERED BY AIRAVATA

© 2026 AXIOMAERA PVT. LTD. · ALL RIGHTS RESERVED
*All logos & brand names are property of Axiomaera. Unauthorised reproduction will lead to legal consequences.*