

CRS Fraud Finder

Powered by AtData

How CRS Fraud Finder Solves the Real Problems You Face

USE CASE #1

Validate Customer Identity at Sign-Up

#Fintechs

#Marketplaces

#Lenders

PROBLEM

Fake accounts with synthetic identities inflate operational costs and risk.

SOLUTION



Use email-based identity verification to confirm email legitimacy at sign-up.

Why it matters: Use email-based identity verification to confirm email legitimacy.

Key signals used: Email age, validation, first seen date, behavioral patterns.

USE CASE #2

Improve Approval Rates for Legitimate Users

#RiskTeams

#ProductManagers

#GrowthManagers

PROBLEM

Overly cautious systems block good users, causing drop-off and churn.

SOLUTION



Leverage nuanced email signals to approve real users with confidence.

Why it matters: Better conversion, less friction, and a better customer experience.

Key signals used: Email popularity, validation confidence, prior usage.

USE CASE #3

Detect and Block Synthetic Identities

#ConsumerLenders

#BNPLplatforms

#DigitalBanks

PROBLEM

Fraudsters create lifelike but fake personas that evade traditional KYC.

SOLUTION



Analyze email longevity and use history to catch synthetic profiles.

Why it matters: Saves money on fraud payouts and protects your reputation.

Key signals used: Email frequency, usage across digital platforms, anomalous behavior.

USE CASE #4

Stop Transactional Fraud and Chargebacks

#eCommerce

#DigitalGoods

PROBLEM

Fraudulent purchases lead to chargebacks, fees, and losses.

SOLUTION



Run risk checks on the customer's email address at checkout.

Why it matters: Block transactions from risky emails before the fraud happens.

Key signals used: Domain reputation, velocity, fraud consortium data, IP matching.

USE CASE #5

Flag Risky Account Updates in Real-Time

#PaymentGates

#UserAccounts

#SavedPaymentMethods

PROBLEM

Fraudsters hijack accounts by changing credentials.

SOLUTION



Evaluate the risk level of every new email submitted to your system.

Why it matters: Catch takeover attempts before accounts are compromised.

Key signals used: Change frequency, mismatched user history, risk scoring on new inputs.

Interested in CRS Fraud Finder?

Contacts us and get access today!



Jay Shah

Director of Strategic Partnerships
jay.shah@crscreditapi.com
+1 551-216-8505



CRS Group, Inc.
www.crscreditapi.com