



Email risk search

Assess risk using email address metadata

Powerful data point for fraud prevention

Email addresses are a unique global identifier and rich with transaction history



What is Email Risk search?

The Email Risk search uses your customer’s email address to search a blacklist of known or highly suspicious email, IP address, domain and phone data. The search also uses email address metadata and active intelligence to reveal fraud and risk patterns.

From this search you will receive a predictive risk score for each customer, plus details of any risk and fraud signals. The score continuously improves over time as fraud events are shared, delivering a state of continuous intelligence.



Available exclusively via IDMatrix

If you’re an IDMatrix customer, you can ‘switch on’ access to the Email Risk search. This means you will be able to perform the Email Risk search as part of your existing IDMatrix call. Search results will be incorporated into IDMatrix decisioning, configured in line with your business and compliance needs.



How does it help me?

It helps you mitigate previously hidden risk at customer acquisition without impacting the customer experience. Because you already capture customer email information, there will be no extra friction or demands on your verification workflows.

Benefits include:



Identifies and prevents fraud



Predictive risk score for each customer



Enables faster, more efficient risk decisions



Delivers a frictionless user experience



How are Email Risk Searches incorporated into IDMatrix business rules?

Business rules within IDMatrix are flexible and can be changed over time, such as when a new data set becomes available or your business or compliance needs evolve. Choose from one or more of the following options when deciding how to incorporate Email Risk search:



AS PART OF KNOW
YOUR CUSTOMER (KYC)

Contributing a name match
to ID verification rules



AS PART OF THE FRAUD
ASSESSMENT MODULE

Incorporate any one or some of the following
fraud signals from the response:

- Risk levels for email address, domain or IP
- Email age
- Digital identity score



What input is required?

The Email Risk Search requires this
information about your customer:

- ✓ Email address
- ✓ Name
- ✓ Address
- ✓ IP Address
- ✓ Phone number

*Email address is the
only compulsory input*



What results are returned?

Over 130 high value response elements are
returned relating to risk and fraud signals

How to get started?

Contact your Equifax Account
Manager or email our team



13 8332



salesau@equifax.com