AtData
THE EMAIL ADDRESS EXPERTS

AtData Fraud Services API

Introduction

AtData’s Fraud API provides detailed information about every email address and its level of risk and fraud correlation. This information is made available due to the billions of activity events AtData observes each month, our vast historical email database and our fraud consortium database.

Fraud Prevention API Endpoint

The endpoint to obtain data using email address is:

> ⓘ https://api.atdata.com/fr

Query Parameters

The query parameters for the Fraud Prevention API are shown in the table below.

Parameter	Required	Description
email	Yes	The email address that is to be evaluated for fraud. The value should be URL encoded.
reference_id	No	Your internal identifier for the email or the transaction it pertains to. This may be used to cross reference results with the AtData Feedback API. The value should be URL encoded.
first	No	First name
last	No	Last name
street	No	First line of the postal address (including number)
city	No	City of the postal address
state	No	State of the postal address
zip	No	ZIP or postcode of the postal address
country	No	2 letter country code of postal address following ISO 3166 standard alpha-2 code (e.g. "US", "CA")
phone	No	Phone number, including country code
ip	No	User's IP address
user_agent	No	User agent

Example API Request

An example of a Fraud Prevention query:

> ⓘ https://api.atdata.com/fr?email=demo%40atdata.com&reference_id=a4840850-98be-46de-b391-3d52732d27c4&first=Joe&last=Bloggs&street=123%20Main%20St&city=New%20York&state=NY&zip=P2P6%2B3P&phone=16467421771&ip=1.2.3.4&user_agent=python-requests%2F2.27.1&api_key=1234567890abcdef

Replace 1234567890abcdef with your API key.

API Response Overview

If your API request is properly formatted and your API key is configured for Fraud Prevention, the API response will contain the below sections in JSON format:

```
{
    “risk”: {
        “query_id”: “2744dd5d0acb475b81687d366fff4c48”,
        “score”: 50,
        “tumbling_risk”: 0,
        “ip”: {
            “routing_type”: “fixed”,
            “organization”: “atdata”,
            “proxy_type”: “tor”,
            “hosting_facility”: true,
            “latitude”: 38.89768,
            “longitude”: -77.03651
        },
        “domain”: {
            “domain_risk_score”: 5
        },
        “postal”: {
            “first_name_match”: “match”,
            “last_name_match”: “no_match”,
            “street_match”: “no_data”,
            “city_match”: “no_data”,
            “zip_match”: “no_data”,
            “deliverability”: “undeliverable”,
            “deliverability_substatus”: “missing_primary”,
            “address_type”: “Street”
        }
    },
    “eam”: {
        “date_first_seen”: “2016-08-09”,
        “longevity”: 3,
        “velocity”: 10,
        “popularity”: 10
    },
    “dam”: {
        “date_first_seen”: “2002-11-09”,
        “longevity”: 3,
        “velocity”: 10,
        “popularity”: 10
    },
    “email_validation”: {
        “status”: “valid”,
        “status_code”: 50,
        “domain_type”: “freeisp”
    }
}
```

The response is composed of four JSON objects that contain related sets of information. A description of each section and the fields it contains can be found in the below tables.

Risk Fields

The AtData risk fields leverage our historical database and the billions of email events we see each month to assess the correlation of the input email to fraud.

Field Name	Value	Description
score	0 - 100	A machine learning-based score of 0 – 100 using AtData's metadata, of which the API response is only a part, to identify high risk and fraudulent profiles. A score of 0 being low risk and 100 being very high risk. The average risk threshold is from 70 – 80 but depends on customer requirements.
tumbling_risk	0 - 3	A score indicating multiple variations of the same email address (e.g. jondoe@gmail.com and jon.doe+123@gmail.com are identical to gmail). 0 indicates no tumbling detected, while values of 1, 2 and 3 indicated a linear risk of tumbling detected. Tumbling is evaluated across AtData's entire network, not just your own activity.
query_id	36 character string	AtData's unique identifier for the response provided. Can be used with our Feedback API or for troubleshooting.

IP Insights Fields

Information about the IP address provided.

⚠ If IP is not provided in the request, the ip object in the response will be null.

Field Name	Value	Description
routing_type	See list of routing types below	The IP Routing Type (IPRT) specifies how the connection is routed through the Internet and can be used to determine how close the user is to the public IP address. For example, a user connecting through a fixed connection is likely very close to the connection. A user connecting through a regional proxy is probably in the same country as the connection, whereas a user connecting through a satellite connection could be anywhere.
Organization		Registering Organizations include many types of entities, including corporate, government, or educational entities, and ISPs managing the allocation and use of network blocks.
proxy_type	http, service, socks, socks http, tor, unknown, web, privacy proxy	The network or protocol utilized by the server to proxy the user connection is identified. Proxy type classifications include the use of http, Tor, web and SOCKS.
Hosting Facility	True/false	Hosting facility includes the following type of service providers: colocation, cloud computing, dedicated hosting, virtual private servers and web hosting. A value of "true" indicates that the IP address is associated with a hosting facility; otherwise the value is "false"
Latitude	Float	Latitude of the identified location, expressed as a floating point number with range of - 90 to 90, with positive numbers representing North and negative numbers representing South.
Longitude	Float	Longitude of the identified location, expressed as a floating point number with range of -180 to 180, with positive numbers representing East and negative numbers representing West.

IP Routing Type	Description
fixed	The user is connecting through a fixed-line connection, such as cable, DSL, T1, and fiber. The user is likely to be at or near the location assigned to the IP.
aol, aolpop, aoldialup, aolproxy	The user is part of the AOL network. AtData can identify the user country in most cases. However, establishing the user location below country is not possible.
pop	The user is dialing into a regional ISP (Internet Service Provider) and is likely to be near the IP location.
satellite	The user is connecting to the Internet through a consumer satellite or a backbone satellite provider, where no information about the terrestrial connection is available. The user can be anywhere within the beam pattern of the satellite, which can span a continent or more.
cache proxy	The user is using a proxy connection, either through an Internet accelerator or a content distribution service. It is possible the user is located in a different country from the IP location.
international proxy	The user is connecting through a proxy (not an anonymizer) that routes traffic from multiple countries. It is possible the user is located in a different country from the IP location.
regional proxy	The user is connecting through a proxy (not an anonymizer) that routes traffic from multiple states within a single country. It is possible the user is located in a different state from the IP location.
corp proxy	The user is connecting through a proxy (not an anonymizer) that routes traffic through edge nodes, or nexus points for traffic entering and exiting a corporate network.
mobile gateway	The user is using a gateway to connect mobile devices to the public Internet. Many mobile operators, especially in Europe, serve more than one country and backhaul traffic through centralized network hubs. Therefore, it is possible the user is located in a different country from the IP location.

Domain Risk Score

Field Name	Value	Description
domain_risk_score	0 - 10	The domain risk score allows users to identify high risk email domains the moment they first appear rather than waiting for industry classification. It encompasses different types of risky domains and their behaviour derived from the AtData network. Score of 0 means there is no risk associated with the domain, a score of 10 indicates that the domain poses a significant threat due to multiple variables.

Email to Postal Correlation Insight Fields

⚠ If no name or postal fields are provided in the request, the postal object in the response will be null.

Field Name	Value	Description
first_name_match ⚠ If first is not provided in the request, first_name_match will be null.	Match no_match no_data	Checks to see if the First Name matches first names previously associated with that email. Results include “match” = First name supplied matches first name previously associated with email “no_match” = First name supplied does NOT match first name previously associated with email “no_data” = No First Name records associated with that email

Field Name	Value	Description
last_name_match ⚠ If last is not provided in the request, last_name_match will be null.	Match no_match no_data	Checks to see if the last name matches last names previously associated with that email. Results include “match” = Last name supplied matches Last Name previously associated with email “no_match” = Last name supplied does NOT match Last Name previously associated with email “no_data” = No Last Name records associated with that email
street_match ⚠ If street is not provided in the request, street_match will be null.	Match no_match no_data	Checks to see if the street matches streets previously associated with that email. Results include “match” = Street supplied matches previously associated with email “no_match” = Street supplied does NOT match street previously associated with email “no_data” = No Street records associated with email
city_match ⚠ If no postal fields are provided in the request, city_match will be null.	Match no_match no_data	Checks to see if the city matches city data previously associated with that email. Results include “match” = City supplied matches city previously associated with email “no_match” = City supplied does NOT match city previously associated with email “no_data” = No City records associated with that email
zip_match ⚠ If no postal fields are provided in the request, zip_match will be null.	Match no_match no_data	Checks to see if the zip matches zip data previously associated with that email. Results include “match” = Zip supplied matches zip previously associated with email “no_match” = Zip supplied does NOT match zip previously associated with email “no_data” = No Zip records associated with that email
address_type ⚠ If no postal fields are provided in the request, address_type will be null.	• Alias • Firm • General Delivery • Highrise • PO Box • Rural Route • Street	The type of the address.

Field Name	Value	Description
deliverability ⚠ If no postal fields are provided in the request, deliverability will be null.	deliverable undeliverable possibly_deliverable probably_deliverable	Postal address deliverability status by the US Postal Service.
deliverability_substatus ⚠ If no postal fields are provided in the request, deliverability_substatus will be null.	23+ possible values. The most common 5 are: • deliverable (deliverable) • missing_secondary (possibly_deliverable) • missing_primary (undeliverable) • maildrop_or_inactive (probably_deliverable) • invalid_street (undeliverable)	Primary reason for the deliverability status.

Email Activity Metrics (EAM) Fields

The origin of AtData’s fraud solution is our Email Activity Metrics, which are used by all the leading antifraud solutions that evaluate email addresses. Through our broad client base, our extensive partner network and our 20-year history, AtData has the highest recognition rate of U.S. email addresses in the market, over 98%.

Forty percent of fraudsters use new email addresses. If AtData does not recognize an email address or only recently encountered it, beware.

Field Name	Value	Description
date_first_seen	YYYY-MM-DD or "now"	The date the email address first appeared in AtData's records. The value “now” will be returned if the email address is new to AtData.
longevity	0 - 3	A score describing when AtData first encountered the email address: 0 = AtData has not encountered this email address before 1 = AtData first encountered this email within the last month 2 = AtData first encountered this email within the last year 3 = AtData first encountered this email over a year ago
velocity	0 - 10	A score reflecting the activity of the email address over the last 6 months, from 0 (no activity) to 10 (most active).
popularity	0 - 10	A score gauging the popularity of the email address over the last 12 months based on the number of sources from which AtData has received the address, from 0 (no sources in 12 months) to 10 (most sources).

Domain Activity Metrics (DAM) Fields

Similar to the EAM fields, the Domain Activity Metrics reflect activity at the domain level. Again, new or recent domains are more risky.

Field Name	Value	Description
date_first_seen	YYYY-MM-DD	The date the domain first appeared in AtData's records. The value “now” will be returned if the domain is new to our database.
longevity	0 - 3	A score from 0-3 indicating when AtData first encountered the domain.
velocity	0 - 10	A score reflecting the activity of the domain over the last 6 months, from 0 (no activity) to 10 (most active).
popularity	0 - 10	A score gauging the popularity of the domain over the last 12 months based on the number of sources from which AtData has received the address, from 0 (no sources in 12 months) to 10 (most sources).

Email Validation Fields

AtData's industry-leading email validation service is used by retailers, data companies and marketing platforms to verify whether an address can receive email or not and whether mailing to that address will affect the sender's ability to deliver email messages into the inboxes of its customers. AtData email validation stops invalid, misspelled and fake emails as well as emails that put your email marketing program at risk, such as spam traps.

Email Validation has a different purpose than fraud prevention, but if an email address is flagged with an "invalid" status, it should be rejected. However, a validation status of "risky" indicates that the email presents risk to your email marketing program, not that it presents risk of fraud. Full documentation of our validation API, including multiple examples, is located at https://docs.atdata.com/#emailvalidation-introduction.

Field Name	Value	Description
address		Contains the email address you queried with in a standardized format.
status	See table below	The summary status of the email validation result.
status_code	See list of values	A range from 5-999 will always be returned and describes the detailed results of the validation within the "status" categorization.
domain_type	See table below	An optional field, domain_type indicates the type of the domain including, "disposable", "freeisp", etc.
role_account	true	An optional field, role_account is returned if the email address is identified as the role related email account. A role account is an email address for a business job role or a group of people in a company such as sales, info, support, marketing or customer service (e.g. info@abc.com).

Email Status Values

The table below lists the possible values for the "status" field in the "email_validation" response.

Field Name	Description
valid	The email address passed all checks and is safe to mail.
invalid	Do not mail. The email does not have proper syntax, the domain is dead or the mailbox doesn't exist.
risky	The email address is valid but it may cause delivery issues (e.g. spamtrap, honeypot or complainer). If you're having deliverability issues, don't send email to risky addresses. *Note: In the context of email validation, "risky" does not mean increased chance of fraud.*
unverifiable	The domain doesn't support a mailbox level check. Also known as an "accept all" or "catch all" domain. Expect some bounces from these addresses should you choose to mail them.
unknown	The syntax and the domain of the email are valid, but we could not confirm the mailbox in the time allowed. Messages to these addresses may see bounces. Repeating the query later may deliver a valid/invalid status.

Domain Type Values

The “domain_type” field will be present in the “email_validation” response if the type of domain has been categorized. The table below shows the full list of domain types and their descriptions.

Domain Type	Description
biz	The domain of a corporation or business.
disposable	The domain is used to create temporary email addresses. AtData assigns these domains an “invalid” status.
edu	An educational institution.
freeisp	A free Internet Service Provider.
gov	A governmental institution.
paidisp	An Internet Service Provider that requires a paid subscription to create an email address.
parked	The domain does not have an active website.
privacy	The domain is used to protect the privacy of the user, e.g. Apple’s Mail Privacy Protection.
wireless	Domains for wireless devices that the must not be sent unsolicited emails, as per the FCC.

Feedback API

When fraud is identified, this information can be shared with AtData through the Feedback API. The benefit to this is that AtData can use past fraud reports to prevent future fraud from the same source. It also helps in the training of our models so that new fraud trends are identified and accounted for in our logic. If you are notified of confirmed fraud, submit this information through the feedback API.

Getting started

To submit data to the feedback API, submit a HTTPS POST request to the /feedback/v1 endpoint. Include a **tab-separated file** with the following fields:

Field	Required?	Description
query_id	Y*	The UUID from the original query to the fraud API (if applicable)
reference_id	N	Client’s own reference Id
email	Y*	Email address
md5_email	Y*	MD5 email address
first	N	First name
last	N	Last name
street	N	Address line 1
street2	N	Address line 2
city	N	City

Field	Required?	Description
state	N	State
zip	N	Zip code
ip	N	IP address
phone	N	Phone number
risk_level	Y	High/Medium/Low
risk_type	N	Category of risk or fraud identified by the client: • credit card • chargeback • account takeover • synthetic identity • loan • refund • gambling • friendly fraud • account abuse • other
source	N	How the feedback was determined: • rule • manual review • chargeback
time	N	The date the fraud occurred in ISO-8601 format with time and time zone. E.g. 2022-01-01T13:26:59+00:00
comment	N	Optional text field providing context to the risk level for use in analysis, reporting and modelling.

Risk_level and one of query_id, email, or md5_email are compulsory fields.

Examples

> ⓘ 00000000000000000000000000000000 is a fake API key and should be replaced with a genuine fraud API key for these commands to work.

File feedback.tsv

```
reference _ id                        email                       ip              risk _ level  risk _ type    source
453127da-9020-4bc5-87b9-30317b8be0d0  fraudster2023@atdata.com    19.172.217.255  High          credit _ card  chargeback
9be3edef-9244-4597-baf9-36ebfc271f4d  up.to.no.go.od@gmail.com    113.214.70.139  High          credit _ card  chargeback
```

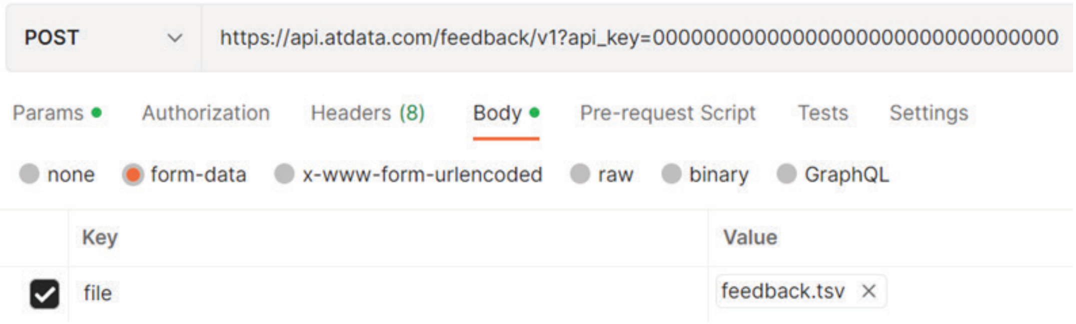
Python

```
import requests

API = ‘https://api.atdata.com/feedback/v1’
# Replace this with the API Key used for the Fraud API
YOUR _ API _ KEY = ‘00000000000000000000000000000000’

with open(‘feedback.tsv’, ‘rb’) as infl:
    files = {‘file’: infl}
    resp = requests.post(f’{API}?api _ key={YOUR _ API _ KEY}’, files=files)
```

Curl

```
curl -F ‘file=@feedback.tsv’ https://api.atdata.com/feedback/v1?api _ key=00000000000000000
000000000000000
```

Postman



POST https://api.atdata.com/feedback/v1?api_key=00000000000000000000000000000000

Params ● | Authorization | Headers (8) | Body ● | Pre-request Script | Tests | Settings

○ none ● form-data ○ x-www-form-urlencoded ○ raw ○ binary ○ GraphQL

	Key	Value
☑	file	feedback.tsv ×