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.towerdata.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 that was received
"last"	No	Last Name that was received
"street"	No	First line including number of the address
"city"	No	City of the address given
"state"	No	State of the address given
"zip"	No	ZIP or postcode of the address given
"phone"	No	Phone Number given including country code
"ip"	No	Users IP collected
"user_agent"	No	User Agent data collected

Example API Request

An example of a Fraud Prevention query:

```
https://api.towerdata.com/fr?email=demo%40towerdata.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": {
                "score": 22,
                 "query_id": "906fa61b-a0d8-42a4-af3d-bd05f6520876"
                 "tumbling_risk": 1,
                "ip_routing_type": string,
                 "organization": string,
                 "proxy_type": string,
                 "hosting_facility": boolean
        },
        "eam": {
                "longevity": 3,
                "velocity": 0,
                "date_first_seen": "2011-08-01",
                "popularity": 0
        },
        "dam": {
                "longevity": 3,
                "velocity": 0,
                "date_first_seen": "2008-05-28",
                "popularity": 0
        },
         "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.

Email Activity Metrics (EAM) Fields

The origin of AtData's fraud solution is our Email Activity Metrics, which are used by all the leading anti-fraud 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	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.towerdata.com/#email-validation-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.

Status	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.

IP Insights Fields

Field Name	Value	Description
IP 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”

IP Routing Type	Description
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. The specific values reflect specific functions within the AOL network. For most commercial applications, all these values indicate only that the IP address is part of the AOL network
pop	The user is dialing into a regional ISP (Internet Service Provider) and is likely to be near the IP location. Note, however, that the user might be dialing across geographical boundaries
satellite	connecting through a consumer satellite service, refer to connection_type field.
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.