MAXMIND

minFraud Insights Data Dictionary

Using Insights to Assess Risk

As a minFraud Insights customer you have access to a broad array of data points, giving you the information you need to make informed assessments about the risk of your transactions.

Insights data can help you understand the risk related to a customer's IP address, email address, device, credit card, and physical addresses.

The following dictionary contains information about a subset of the minFraud Insights outputs that we have identified as particularly useful for assessing different kinds of risk.

Contents

IP Address

minFraud provides data points related to the stability and legitimacy of a customer's IP address. You can use minFraud's data to help you understand whether a customer is using an anonymizer and what type of anonymizer they are using. Beyond anonymizers, the IP data in minFraud can be used to better understand the context of a transaction: whether your customer is acting on behalf of a business, how stable their IP address is, and whether they are conducting their transactions while traveling.

IP Geolocation

Several data points give a comprehensive picture of the geolocation of the IP address associated with the transaction. Many of these data points are self-explanatory, but if something doesn't seem right, you may consult the data points below for better context.

Insights Data	Assessing Risk

`country/confidence`
`city/confidence`
`subdivisions/confidence`
`postal/confidence`
	If the IP geolocation does not seem to correspond to a location that makes sense for your business, or for the specific customer involved in the transaction, you can check our IP geolocation confidence values. It may be that we are less confident of the geolocation in this particular circumstance. If so, this may decrease the risk of an geolocation mismatch.

`location/accuracy_radius`	As with confidence factors, the accuracy radius of the IP geolocation can be used to give you some context about the IP geolocation. If the location for the transaction is within the accuracy radius multiplied by two, this suggests the location matches the expected geolocation.
`location/latitude`	Remember when referencing the latitude

`location/longitude`	and longitude of the IP address that IP geolocation can never locate individual households or street addresses. The latitude and longitude returned as part of your minFraud response will be located near a population center, but will not be the specific coordinates of an IP address. You can use these coordinates for various kinds of distance calculations, but be sure to check the confidence values and accuracy radius to ensure validity.

`registered_country`
 	
`represented_country`
	The information in these fields can help you understand whether the IP address associated with the transaction originates from a military base, or ISP whose national affiliation is different from its location. If you do not expect or cannot do business with a particular country, this may help you flag transactions.

IP Anonymizers

Several data points give a comprehensive picture of customers' use of IP anonymizers.

Insights Data	Assessing Risk
`is_anonymous`	Some customers use IP anonymizers when conducting legitimate transactions, but for many businesses anonymized IP addresses are an indicator of increased risk.
`is_anonymous_vpn`	VPNs are one of the most popular anonymizers. Security conscious customers may use VPNs as a matter of course, while others may be trying to hide their IP address for the purposes of fraud.

`is_hosting_provider`	Web hosting services can be used to create private proxies, and many VPN services use hosting providers to host their services instead of registering their own IP ranges.
`is_public_proxy`	Public proxies tend to be easy to access and are often visibly published.
`is_residential_proxy`	Residential proxies are harder to detect than other kinds of proxies as these IPs appear to be associated with legitimate residential ISPs.
`is_tor_exit_node`	These are published IPs used as exit nodes for the TOR network. Traffic from these nodes have been relayed through several servers to preserve anonymity.

IP Traits

In addition to providing information about anonymizers, there are a number of data points that give you a richer understanding of customers' connections.

Insights Data

`static_ip_score`

Assessing Risk

IP addresses may be frequently moved or reassigned by ISPs. This data point provides a rating of how static the IP address appears to be. The value ranges from 0 to 99.99 with higher values meaning a greater static association.

Many IP addresses with a `user_type` of `cellular` have a score under one since cellular IPs typically serve multiple on-the-move users over a larger area . Broadband IPs associated with a residential connection that don't change as often typically have a score above

	thirty. This can be useful for deciding whether an IP represents the same user over time.
user_count	This provides the number of distinct users sharing the IP address or network over the past 24 hours. A higher value indicates this is a high-volume IP that could be associated with a corporate proxy, carrier-grade NAT, or other types of shared connections. It tells you whether this connection is likely tied to one or few, or many different users.
user_type	We identify the following types of IP user: • `business` • `cafe` • `cellular` • `college` • `content_delivery_network` • `dialup` • `government` • `hosting` • `library` • `military` • `residential` • `router` • `school` • `search_engine_spider` • `traveler` Do you expect transactions to be initiated from travelers or college students? Do you expect customers to initiate transactions from mobile devices? Use this data point with others to ensure that a transaction conforms to expectations.

Email

Several data points related to the email address can be used to help you assess fraud in a transaction.

Email

Insights Data	Assessing Risk
email_domain/first_seen	When the email domain (i.e., @gmail.com, @yahoo.com, etc.) was first seen in the minFraud network. Customers with email address domains that have only recently been seen may not conduct many transactions, or the domain could be new. Alternatively, this could indicate a fraudster creating a new email domain to fake being a legitimate business or to avoid having a history of use.
first_seen	When the email address was first seen in the minFraud network. An email address that has been around, conducting transactions for a long time may be more trustworthy than a new email address. If the email has been around longer, this may also correlate to a more accurate determination of whether the email `is_high_risk` (see below).
is_disposable	Disposable or temporary email addresses are sometimes used for privacy or to prevent spam, but they can also be used by fraudsters to avoid detection as there is no history of use to draw from to inform risk scoring.
is_free	Use of free email providers (e.g. Gmail,

	Yahoo, Outlook, etc.) by consumers is the norm, so this data point is often only in business-to-business contexts where a business email/domain is sought after.
`is_high_risk`	Based on the email address's activity in the minFraud network, whether we believe that the email is high risk.

Device

If your minFraud integration is set up to include device tracking, then your API responses will include important information about the device that may be helpful for assessing the riskiness of a transaction.

Device

Insights Data	Assessing Risk
`confidence`	This number reflects our confidence that the device which has been identified with the transaction is a unique device as opposed to a cluster of similar devices. If the number is lower, the other data points are less likely to be accurate and should not be used to make a large determination as to risk. If the number is higher, the other data points can be more reliably consulted.
`last_seen`	The time that the device was last seen on your site specifically. Check this value against your local web session logs to confirm that this device is associated with a particular user.
`local_time`	Check the local time of the device making the transaction against the billing address and IP geolocation information to confirm that the device is operating in the location the customer is representing with user-supplied data and the information gleaned from the IP address.

Credit Card

minFraud provides data points related to the credit card used in a transaction. Check the information about the credit card against other details of the customer and their transaction history.

Credit Card

Several data points give attributes of the credit card associated with the transaction. Many of these data points are self-explanatory, but if something doesn't seem right, you may consult the data points below for better context.

Insights Data	Assessing Risk
`brand`	Using the card brand in combination with other data points can help identify fraud trends over time. For example, you may notice a fraud attack coming from Visa prepaid cards or American Express cards from certain countries. These trends may emerge based on the characteristics of stolen cards from data breaches.
`country`	You can check the country in which the credit card was issued against other details from the transaction and customer history. If there is some discrepancy between where the card was issued and where the customer is located, or attempting to ship a product, that may indicate a higher risk.
`is_prepaid`	Customers may use a prepaid gift card for any number of reasons. They are easy to purchase, and can be acquired without linking them to a name, address, and other biographical details. If you are concerned that a customer may be trying to hide their identity and their card is prepaid, that may be an indicator of greater risk.

`is_virtual`	Virtual cards do not have a physical card associated with the card number. Customers may use virtual cards for added security, though they are also popular with resellers who use them to attempt to bypass order limits.

Card Issuer

In addition to data points about the credit card, you may find information about the card issuer that is helpful for assessing fraud.

Insights Data	Assessing Risk
`name`	As with the card's `brand` (see above), you may use the card issuer name along with other data points to identify fraud trends related to the credit card over time.
`matches_provided_name`	Some merchants ask their users to enter in the name of their issuing bank as an additional verification step. If you do this, this output matches the user-entered name with our IIN database.
`matches_provided_phone_number`	Some merchants ask their users to enter in the phone number on the back of their credit card as an additional verification step. If you do this, this output matches the user-entered phone with our IIN database.

Physical Address

minFraud provides data points related to the various locations involved in transactions. This always includes the geolocation of the IP address associated with the transaction, but also includes information about the location of billing and shipping address, as well as credit card bank.

Billing and Shipping Address

The IP geolocation information is paired with key information about the billing and shipping address associated with a transaction to give several important data points that can be used to help you assess risk.

Insights Data	Assessing Risk
`shipping_address/is_high_risk`	Based on the shipping address's activity in the minFraud network, whether we believe that the address is high risk.
`is_postal_in_city`	This data point will tell you whether the postal code for the billing or shipping address is in the city for the address. If it is not, it may be missing from our database, a customer typo, or an indication that the address is not legitimate. We use GeoNames data for the postal-city match, which uses the preferred place name for a US ZIP code. Alternative place names for US ZIP codes may not trigger a match for this field.
`distance_to_ip_location`	For both the billing and shipping address, we provide a data point which tells you the distance in kilometers to the geolocation of the IP address associated with the transaction. If this number is especially high, it may indicate that a customer is traveling, or it may be more indicative of risk. Consider whether this

	behavior is expected for your business, and cross reference this number with the confidence values and accuracy radius for our IP geolocation to get a sense of how accurate this value is for this transaction.
`distance_to_billing_address`	This data point tells you how far the shipping address is from the billing address. When this number is high it may indicate that a customer is shipping something to a friend, family, or business. Check other details of the transaction to confirm.
`is_in_ip_country`	For both the billing and shipping address, these data points will tell you whether the address is in the same country as the geolocation we have provided for the IP address associated with the transaction. If the transaction appears to have been initiated in a different country from the billing address, the shipping address, or both, it may be an indicator of increased risk. Remember to cross reference this data point with the country confidence factor for IP geolocation of the specific transaction.