Address Risk API 4.1
Data Dictionary

Document History

Date	Changes
8 September 2024	**Update:** Moved disclaimer for usage of Identity Risk Model to a separate page. Updated Formatting of the document.
30 December 2024	**Major:** Redesign

Table of Contents

Data Dictionary Overview

The following data dictionary provides information to help you understand what each of the response attributes mean, their field values, and how to assess the risk based on the attribute output in relation to your customer's data.

Note: Any attribute that lists a numeric range for field values, specific thresholds may vary by customer.

Definition & Assessing Risk

Validity Level

Definition

- This insight comes from the Identity Network's Validity Insights, which is sourced from authoritative data providers.
- This insight indicates the level to which the input physical address could be validated. For example, if the address was only valid to the city level but not the house level, it would return "valid_to_city".

Assessing Risk

Field Values	Good Consumers	Fraudsters
Missing_address: Where the address is not provided. Neutral risk (generally addresses are either always or never submitted, based on the type of transaction) *Invalid*: medium-high risk *Valid_to_country*: medium-high risk *Valid_to_city*: medium-high risk *Valid_to_street*: neutral risk *Valid_to_house_number*: neutral risk *Valid_to_house_number_missing_apt*: neutral risk	**Behavior:** Enters their real complete billing or shipping address, except in cases they only need to submit a partial address, e.g. postal code. In rare cases they may omit their apartment number. Typos are relatively frequent. **Ekata data:** Usually fully validates the address but occasionally identifies it as invalid or only partially valid.	**Behavior:** For billing, enters the victim's real complete billing address, except in cases where they only need to submit a partial address, e.g. postal code, or in cases where they do not have the full address. If they do not have the full address, they may fabricate an address that includes the details they do have. For shipping, prefers to ship to vacant addresses, commercial mail drops, hotels, or other locations they can pick up from safely without compromising their identity. Some fraudsters will enter the victim's billing address or a fake address and then talk to the shipper to change the location after the order is fulfilled. **Ekata data:** Often fully validates the address, but also commonly identifies it as invalid or only partially valid.

Street Line 1, Street Line 2, City, Postal Code, Zip4, State Code, Country Code

Definition

- This insight comes from the Identity Network's Validity Insights, which is sourced from authoritative data providers.
- These 7 attributes return the normalized and structured address, parsed from the input address.
- Not all fields will have a response, depending on the address. For example, zip4 is used primarily in the US, and countries that don't have states will not return a state code.

Assessing Risk

Field Values	Good Consumers	Fraudsters
Will return a complete address (all applicable fields returned) if fully validated, otherwise will return a partial address with some null fields depending on validity level	**Behavior:** Enters their real complete address. In some cases, they may omit their apartment number. Typos are relatively frequent. **Ekata data:** Will usually return a complete, normalized, and structured address that closely or fully matches the input address but occasionally will have a null street line 2 if not applicable or apartment number is missing.	**Behavior:** Enters stolen, manipulated, or fabricated addresses that includes details of an address they do have. **Ekata data:** Will often return a complete, normalized address that closely matches the input address. Will also commonly identify certain fields as null for partially valid addresses.

Latitude / Longitude

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight returns the latitude and longitude coordinates of the input address and includes the accuracy of the coordinates.
- The accuracy of the coordinates will match that of the validity level, e.g., if only valid to state level, the accuracy will say 'state'.

Assessing Risk

Field Values	Good Consumers	Fraudsters
Null: Where the address is not provided or is invalid *Lat/long*: geo-coordinates of the input address *Accuracy*: one of "neighborhood", "country", "postalcode", "Street", "city", "state", or "rooftop"	**Behavior:** Enters their real complete address. In some cases, they may omit their apartment number. Typos are relatively frequent. **Ekata data:** Will typically return geo-coordinates accurate to rooftop, occasionally will be accurate to street if apartment number is not provided.	**Behavior:** Enters stolen, manipulated, or fabricated addresses that includes details of an address they do have. **Ekata data:** Will typically return geo-coordinates accurate to less than rooftop if manipulated or fabricated but will also return geo-coordinates accurate to rooftop if using stolen address data.

First Seen Days

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight indicates the first time the input physical address has been seen in Ekata's Interaction Insights.
- This insight is based on the normalized address (the address returned in the response).

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When input address is missing, invalid, or on provider timeout. Where the address is not provided or is invalid. *0*: Never seen before; Neutral risk *1-7*: High risk *8+*: Slightly lower risk	**Behavior:** Submits their real address, which is typically used online frequently by themselves, other occupants, and previous occupants. **Ekata data:** It is uncommon that we have not seen the address before, although this varies country-to-country. In lower coverage countries, we may have a higher prevalence of never seen addresses. Most commonly we first saw the address over a year ago.	**Behavior:** Billing addresses generally belong to the card holder victim, who may or may not shop online regularly. Shipping addresses are generally places where the fraudster can safely pick up their merchandise without compromising their identity, such as vacant addresses, commercial mail drops, hotels, etc., which are not addresses associated with frequent legitimate purchases. **Ekata data:** It is uncommon that we have not seen the address before. Never seen or only recently seen addresses are much more common among fraudulent transactions.

Last Seen Days

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight indicates the last time the input physical address has been seen in Ekata's Interaction Insights.
- This insight is based on the normalized address (the address returned in the response).

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Where the address is not provided or is invalid. *0*: Never seen before; Neutral risk *1-7*: High risk *8-89*: Slightly lower risk *90+*: Low Risk	**Behavior:** Most online buyers only shop or sign up to accounts once per month or less. Few do so weekly, and very few do so daily. Typically, the same home address is used on all transactions. Usually, each address includes more than one online shopper. **Ekata data:** Most addresses don't show up more than once per week in our Network. Frequency around one month is the most common. Daily frequencies are rare.	**Behavior:** For billing addresses, fraudsters are typically using a victim's address and will make frequent transactions with it in a short period of time. For shipping addresses, fraudsters prefer vacant addresses, commercial mail drops, hotels, or other locations which they can retrieve packages from, but which are not associated with their identity. This can cluster fraud transactions among a smaller set of addresses than we see in good transactions. **Ekata data:** Addresses show up relatively frequently in our network. A fraudulent online interaction often has an address seen in the last day, or in the last few days. It would be uncommon for the address to not have been seen for months.

Popularity

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight indicates how many merchants have been seen with a unique address over the past 90 days in Interaction Insights.
- This insight is based on the normalized address (the address returned in the response).

Assessing Risk

Field Values	Good Consumers	Fraudsters
0: Never been seen before; neutral risk *1*: Low risk *2-4*: Neutral risk *5-9*: Medium-high risk *10+*: High risk	**Behavior:** Shops on a relatively small number of sites based on their needs and interests. **Ekata data:** Returns a low popularity value.	**Behavior:** Shops on a wide variety of sites based on how easy it is to submit fraudulent transactions, as well as to avoid detection and to mitigate the impact of being blocked on any one website. **Ekata data:** Returns a high popularity value.

Velocity

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight indicates the max number of times a unique address has been seen in Ekata's Identity Network over the last 90 days.
- This insight is based on the normalized address (the address returned in the response).

Assessing Risk

Field Values	Good Consumers	Fraudsters
0: Never been seen before; neutral risk *1*: Low risk *2-4*: Neutral risk *5-9*: Medium-high risk *10+*: High risk	**Behavior:** Typically, only transact or create accounts once a month or less. Few have weekly or daily online interactions. **Ekata data:** Returns a low popularity value.	**Behavior:** Takes advantage of victim's personal information to shop or frequently open fraudulent accounts. **Ekata data:** Returns a high velocity value.

Volatility

Definition

- This insight comes from the Identity Network's Interaction Insights, which is sourced from Ekata's global customers.
- This insight indicates the count of unique identity inputs paired with an address in the last 90 days in our network.
- This insight is based on the normalized address (the address returned in the response).

Assessing Risk

Field Values	Good Consumers	Fraudsters
0: Neutral Risk *1-2*: Medium-High Risk *3-5*: High Risk *6+*: Very High Risk	**Behavior:** Use the same set of identity data consistently. May sometimes use secondary identity elements in place of their primary (e.g. landline instead of their phone, or a work address instead of billing) in online transactions or signups. **Ekata data:** Returns a low volatility score.	**Behavior:** Match victim cardholders' names and addresses with burner phones, throwaway emails, and other temporary identity elements that they change frequently. **Ekata data:** Returns a high volatility value.

Input Completeness

Definition

- This insight comes from the Identity Network's Validity Insights, which is sourced from authoritative data providers.
- This insight indicates the input completeness for the address provided by the customer.

Assessing Risk

Field Values	Good Consumers	Fraudsters
Partial: medium risk *Missing*: no address inputted *Complete*: neutral risk	**Behavior:** Enters their real complete address. In some cases, they may omit their apartment number. Typos are relatively frequent. **Ekata data:** Will usually return a "complete" response. Very rarely will return partial/empty/missing	**Behavior:** Enters stolen, manipulated, or fabricated addresses that includes details of an address they do have. **Ekata data:** Will often return a "complete" response and occasionally will return "partial" if parts of the address are missing.

Address Risk Score

Definition

- This insight is a holistic risk assessment of an address based on the normalized address and returns a score between 0 and 1 rounded to three decimal places.
- A higher score indicates a riskier transaction.
- The address needs to be validated to at least the street level to return a score.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Address was not provided or could not be validated to at least the street level. Range: 0.000 - 1.000 *<.44*: Low risk *.45-.79*: Uncertain *>.8*: High risk	**Behavior:** Enters their real complete address, uses it consistently in all online interactions (transactions, applications, etc.). May change addresses frequently if moves frequently, but not typical. Has typical online behavior, e.g., shops online or creates accounts once a month or less. **Ekata data:** Will usually return a low-risk score	**Behavior:** Enters stolen, manipulated, or fabricated addresses that includes details of an address they do have. Will have frequent/abnormal online behavior, e.g., seen very recently and frequently at a lot of merchants and in combination with other identity elements. **Ekata data:** will usually return a high-risk score

Upgrading Score Versions

Ekata provides a transition period to upgrade from the current version to the new release version of models. During the transition period, both model versions are made available for test and validation. At the close of the transition period, the newly released models will automatically become the production model.

Admins can choose which model version outputs are returned in the admin panel at app.ekata.com.

Admins can also choose when to migrate each API key independently.

Your specific score distribution may be impacted with a new version upgrade. To prepare for the transition, Ekata recommends:

- Retuning your rulesets or retraining your fraud model with the new Ekata scores on a historical dataset. Ekata can provide a score backfill file that contains the transaction_ids passed in the original queries along with the new and current scores for a given time.
- Joining the score backfill file with your internal dataset using the transaction_id allows retuning and retraining fraud rulesets with the newer score against known fraud outcome labels.
- Reviewing the score thresholds in your current fraud implementation with the newer score model version to determine if changes are needed.

Disclaimers

This model is designed to be an informational tool only. This model is provided as a rough estimate of authentication-based risk decisioning performance. The analysis performed by this model is a series of general estimates which are based upon the underlying information and assumptions now available. That information may change over time, and the analysis would need to be updated to reflect those changes for the analysis to be useful. The assumptions regarding authorization rates are hypothetical and there can be no guarantee that they will be achieved. Actual results may vary substantially from the figures shown. Mastercard accepts no responsibility for any losses arising from any use of or reliance upon any calculations or conclusions reached using this Model.

MASTERCARD MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT; (B) RELATING TO THE PERFORMANCE OF SMART AUTHENTICATION OR USE OF RISK INFORMATION; (C) THAT USE OF SMART AUTHENTICATION OR RISK INFORMATION SHALL BE UNINTERRUPTED OR ERROR-FREE; OR (D) CONCERNING THE ACCURACY, QUALITY, RELIABILITY, SUITABILITY, OR EFFECTIVENESS OF THE RISK INFORMATION OR ANY OTHER DATA, RESULTS, CONTENT, OR OTHER INFORMATION OBTAINED OR GENERATED BY COMPANY THROUGH ITS USE OF SMART AUTHENTICATION OR ANY RISK INFORMATION. SMART AUTHENTICATION, RISK INFORMATION, AND OTHER MASTERCARD IP IS PROVIDED "AS IS, " WITH ALL FAULTS, KNOWN AND UNKNOWN. THE COMPANY ASSUMES THE ENTIRE RISK ARISING OUT OF ITS USE OF SMART AUTHENTICATION AND ITS USE OF THE RISK INFORMATION UNDER ALL APPLICABLE LAWS, INCLUDING THOSE RELATING TO PRIVACY AND DATA PROTECTION, BANKING, CREDIT, AND ANTI-DISCRIMINATION.