Identity Review API 3.3
Data Dictionary

Document History

Date	Changes
17 Nov 2025	**Update:** Update wording on ERM and update "Primary/Secondary Address Is Valid" definitions and field values.
27 Aug 2025	**Update:** Update Email Risk Score "Good" and "Bad" examples for accuracy.
03 Mar 2025	**Update:** Updated Network descriptions for Interaction and Validity Insights, revised null return values for mailbox velocity.
11 Dec 2024	**Update:** Included Disclaimer for usage of Identity Risk Model.
21 Aug 2024	**Update:** Inclusion of Email Risk Score and mailbox_velocity on pages 42-43. Updated values for Phone Line Type.
24 Jun 2024	**Update:** Format updates, decapitalizing signal values, added Primary/Secondary Email Match to Address section.
2 Apr 2024	**Update:** IP Match to Primary / Secondary Name signal updated (page 35) due to signal deprecation.
6 Feb 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

Primary/Secondary Phone is Valid

Definition

This attribute comes from Validity Insights, which is sourced from authoritative data providers. This attribute returns a true/false response that signals if the input phone number provided is validated by way of association to a valid carrier, and syntactically correct.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When phone number is missing, or validation timed out *true*: Neutral risk *false*: High risk	**Behavior:** Submits their real phone number, which is a normal working phone. **Ekata data:** Identifies the phone number as valid if available.	**Behavior:** Prefers burner phones but may enter the victim's phone number or a fake phone number if they do not expect it to be called or texted. **Ekata data:** May identify phone number as invalid.

Primary/Secondary Phone Country Code

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates the country location of the input phone number, returned as a two-character country abbreviation (e.g., US, CA, SG, DE, etc.).
- This attribute is derived from the latitude and longitude coordinates of the phone number to return the accompanying country.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When input phone number is missing, is invalid, or on provider timeout. Otherwise, will return a two-character country code	**Behavior:** Uses their normal phone number associated with their country of residence **Ekata data:** Returns a country code that matches the country of residence if available	**Behavior:** Prefers proxy IPs or other ways to hide their identity or uses a phone number in conjunction with mismatched stolen identities. **Ekata data:** May return a country code that does not match the country of primary address, or originates from a country associated with higher incidences of fraud (Russian Federation, Algeria, etc.).

Primary/Secondary Phone is Commercial

Definition

- Returns a Boolean indicating whether the phone is associated with a business.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When input phone number is missing, invalid, or on provider timeout. *true*: Phone number is registered to a business. *false*: Phone number is not registered to a business.	**Behavior:** A business uses their business number, and an individual uses their personal number. **Ekata data:** Identifies whether the phone number is associated with a business or an individual.	**Behavior:** Pretends to be a business when an individual or vice versa.

Primary/Secondary Phone Line Type

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute returns the associated line type with the input phone number and how it is used. It returns one of the following values below:

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: when phone number is invalid or line type is unknown (occurs rarely for some international numbers) *landline*: medium-high risk *fixed-VoIP*: medium-high risk *mobile*: neutral risk voicemail: high risk *toll-free*: high risk *premium:* high risk non-fixed-VoIP: high risk other: high risk	**Behavior:** Use their normal personal phone. **Ekata data:** Identifies the phone line type if available when phone number is valid.	**Behavior:** Prefers burner phones which are often non-fixed VoIP or may enter the victim's phone or a fake phone number if they do not expect it to be called or texted. **Ekata data:** Phone line types associated with higher risk will be identified, e.g., non-fixed VoIP, landline, or other non-mobile line types.

Primary/Secondary Phone Carrier

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates the carrier associated with the input phone number. The phone number must be valid for the phone carrier to be returned.
- The coverage is at the MVNO (mobile virtual network operator) level for most countries meaning the value returned is typically the company who is provisioning the number to the end user rather than the major carrier who owns it.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When phone number is invalid, or carrier is unknown Carrier among the top 3 most common for the country: Neutral risk Other carriers: Medium-high risk Carriers associated with burner phones: Very high risk	**Behavior:** Uses their normal personal phone, which is usually a common mobile carrier. **Ekata data:** Usually returns the name of a common phone carrier for the country.	**Behavior:** Prefers burner phones which are often non-fixed VoIP or may enter an impersonated victim's phone or a fake phone number if they do not expect it to be called or texted. **Ekata data:** Often returns the name of a known phone carrier. However, carriers associated with prepaid or VoIP services, occur more frequently.

Primary/Secondary Phone Is Prepaid

Definition

- This feature comes from Validity Insights which is sourced from authoritative data providers.
- This attribute indicates whether the input phone number is associated with a prepaid account.

Assessing Risk

Field Values	Good Consumers	Fraudsters
true: High risk *false*: Low risk	**Behavior:** Uses their normal personal phone, which is usually a common mobile carrier and is not prepaid. **Ekata data:** Usually returns *false*	**Behavior:** Prefers temporary or burner phone numbers which are often prepaid. **Ekata data:** Usually returns *true*

Primary/Secondary Phone Match to Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates if the name associated with the input phone number matches the input name (person or business).

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Where the phone number is invalid, or input name or phone is not provided. *match*: Name linked to phone number matches Input name; low risk. *no match*: Name linked to phone number does not match input name; high risk. *no-name-found*: No name associated with phone number; neutral risk, high risk where coverage is high.	**Behavior:** Submits their real name and real phone number in transactions and generally keeps the same phone number for a long time. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps or family plans where the subscriber's name doesn't match the phone owner's name, etc.	**Behavior:** Prefers burner or throwaway phones that they change frequently. In rare cases may use the victim's phone number if they don't expect it to be called or texted. **Ekata data:** Will very rarely verify the match and often will have no name attached to the phone.

Primary/Secondary Phone Match to Address

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates if the location of the input phone matches the location of the input address.
    - Match: phone location matches input address line 1, address line 2, city, state, and postal code
        - "Match" indicates that we have authoritative data sources telling us that the phone number and address queried together are also attributed/linked to one another. Aside from sources that provide both phone and address matching together, we will also derive a "Match" status if multiple sources can corroborate the match via additional PII linkages.
    - Postal match: phone location postal code matches input address postal code
    - Zip4-match: phone location postal code zip+4 matches input address postal code zip+4. This is more precise than postal match but is only possible if zip4 was passed in the API query
    - City-state-match: phone location city and state matches input address and state
    - Metro-match: phone location is in the same metro area as input address
    - Country-match: phone location country matches input address country
    - No match: phone location does not match input address

Assessing Risk

Field Values	Good Consumers	Fraudsters
match: Low risk *Postal match* or *zip+4 match*: Medium risk *City-state-match* or metro match: Medium risk *Country match*: High risk *No match*: Highest risk. The phone number is normalizing to another country	**Behavior:** Submits their real address and real phone number when opening accounts, and generally keeps the same phone number and address for a long time. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps, subletting, or minors under 18.	**Behavior:** If impersonating a victim, then will typically enter the victim's address, but may falsify the phone number (or vice versa). Fraudsters may also enter a fabricated name and address, or in rare cases use their own real identity data. **Ekata data:** Will do the phone to address match to assess and qualify the risk.

Primary/Secondary Subscriber Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute returns the name of the subscriber

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No phone number was provided. Full Name: A string containing the full name of the phone subscriber.	**Behavior:** Submit a phone number associated with their name. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps or minors under 18.	**Behavior:** Submit fake or false phone numbers, which are not associated with their name. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps or minors under 18.

Primary/Secondary Address Is Valid

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates if the physical address could be fully validated. For example, if the address was only valid to the city level, it would return "false".

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When address is missing, or validation timed out *true*: Neutral risk *false*: High risk	**Behavior:** Enters their real complete billing or shipping address, except in cases where they only need to submit a partial address, e.g., postal code. In rare cases, they may omit their apartment number. **Ekata data:** Most common, validates the full address provided. It may identify it as invalid or partially valid.	**Behavior:** For primary address, fraudsters enter 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 of the victim. If they do not have the full address, they may fabricate an address that includes the details they do have. For secondary address, 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:** May validate the address but may identify it as invalid or partially valid.

Primary/Secondary Address Input Completeness

Definition

- This attribute comes from our Validity Insights, which is sourced from authoritative data providers.
- This attribute 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.

Primary/Secondary Address Match to Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates if the input name matches any of the people or businesses linked to the physical address.
- The address needs to be validated to at least the street level to get a response.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Where the address is not validated to at least street level, Input name is not provided, or address to name coverage is not available. match: Name linked to address matches Input name; medium-low risk. No match: Name linked to address does not match Input name; high risk. No name found: No name associated with address found; neutral risk, high risk where coverage is high	**Behavior:** Submits their real name and real address in transactions, usually without typos, and usually lives at the same address for a year or longer. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps, subletting or minors under 18 years.	**Behavior:** Typically enters the victim cardholder's name and address but may not have the complete address. In this case they may fabricate or find some real address that matches the data they do have. **Ekata data:** Sometimes verifies the match but often will return no match or no name found.

Primary/Secondary Address Resident Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute provides the full name of the resident associated with the input address.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No address was provided. Full Name: A string containing the full name of the resident.	**Behavior:** Submits their real name and real address. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps, subletting or minors under 18 years.	**Behavior:** Typically enters the victim cardholder's name and address but may not have the complete address. In this case they may fabricate or find some real address that matches the data they do have. **Ekata data:** Sometimes verifies the match, but often will return no match or no name found.

Primary/Secondary Address is Commercial

Definition

- Returns a Boolean indicating whether the address is associated with a business.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No address was provided *true: Address is associated with a business address* *false*: *Address is associated with a personal/residential address.*	**Behavior:** When shipping physical goods, commercial addresses are typically a positive signal and indicate that the order is not fraudulent.	**Behavior:** Do not have all the information and often fill in information that results in inconsistencies between whether an entity is a business and whether the address is associated with a business.

Primary/Secondary Address is Forwarder

Definition

- Returns a Boolean indicating whether the address performs freight forwarding or reshipping services.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No address was provided *true*: Address is associated with a location performing freight forwarding or reshipping services. *false*: Address is not associated with a location performing freight forwarding or reshipping services.	**Behavior:** Do not make use of freight forwarding services.	**Behavior:** Make use of freight forwarding services to circumvent import restrictions or their true address.

Primary/Secondary Address Type

Definition

- Indicates the delivery point for the address.
    - Commercial mail drop - private PO boxes, examples include UPS Store and Mailboxes, etc.
    - Multi unit - apartment or office buildings containing multiple separate postal units.
    - Single unit - single family homes or commercial buildings not comprising separate postal units.
    - PO box - post office box where mail can be collected but which is not a residence.
    - PO box throwback - addresses for which mail is forwarded to a PO box.
    - Unknown address type - delivery point is not known.

Assessing Risk

Field Values	Good Consumers	Fraudsters
Commercial Mail Drop: Medium Risk Multi Unit: Low Risk Single Unit: Low Risk PO Box: Medium Risk PO Box Throwback: High Risk Unknown Address Type: Highest Risk	**Behavior:** Have items shipped to their home or business address. **Ekata data:** Can often determine the address type.	**Behavior:** More likely ship to PO boxes or PO box throwbacks to conceal their home address. **Ekata data:** Often identifies as PO Box, PO Box Throwback, or Unknown address type.

Secondary Address Distance from Primary Address

Definition

- This attribute returns an integer indicating the distance between the primary and secondary address in miles

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No secondary and primary address provided 1-9: Low Risk 10-99: Neutral Risk 100+: Higher Risk	**Behavior:** Operate within a smaller geographic region	**Behavior:** Input incorrect or misleading address information

Secondary Address Linked to Primary Resident

Definition

- Returns Boolean indicating whether the secondary address is linked to the primary resident

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: No secondary or primary address provided. *true*: Names match: Low Risk *false*: Names do not match: Neutral Risk	**Behavior:** Are associated with secondary addresses **Ekata data:** Emails may be identified as invalid.	**Behavior:** Provide false or misleading address information.

Primary/Secondary Email is Valid

Definition

- This attribute returns a true/false response that signals whether the input email is a valid email address or not.
- This attribute is from Identity Network's Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing *true*: Neutral risk *false*: High risk	**Behavior:** Submits their real email address, which is a normal working email **Ekata data:** Emails may be identified as invalid.	**Behavior:** Prefers temporary or newly created emails or may enter a fake email if they do not expect it to be verified. **Ekata data:** Emails may be identified as valid

Primary/Secondary Email is Autogenerated

Definition

- This attribute returns a true/false response that signals whether the input email is from a known auto generated source or not.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing *true*: Medium Risk *false*: Low Risk	**Behavior:** Submits their real email address, which is a normal working static email. **Ekata data:** Identifies the email as autogenerated or not if available in Ekata's Network.	**Behavior:** Prefers auto generated emails. **Ekata data:** Emails may be identified as autogenerated

Primary/Secondary Email is Disposable

Definition

- This attribute returns a true/false response that signals whether the input email is from a known disposable domain or not.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing *true*: High Risk *false*: Low Risk	**Behavior:** Submits their real email address, which is a normal working static email. **Ekata data:** Identifies the email as disposable or not if available in Ekata's Network.	**Behavior:** Prefers temporary disposable emails. **Ekata data:** Emails may be identified as disposable.

Primary/Secondary Email First Seen Days

Definition

- This attribute comes from Validity Insights, which is sourced from Ekata's global customers.
- This attribute indicates the first time that the input email has been seen in Interaction Insights.
- The email address does not need to be active for it to be in Interaction Insights.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing 0: Never seen before, high risk 1-90: Very high risk 91-365: Neutral risk 366+: Low risk	**Behavior:** Submits their real email address, which is typically used online frequently. **Ekata data:** Likely first saw the email a long time ago. Some emails have never been seen where coverage is low. Emails seen only recently are less common, since consumers do not change emails often.	**Behavior:** Typically utilizes disposable or temporary emails and change email addresses frequently. If they are impersonating a victim, they rarely use the victim's email unless they have gained full login access. **Ekata data:** Likely have never seen the email before or have seen it only recently. Emails first seen a long time ago are unlikely.

Primary/Secondary Email Domain Creation Days

Definition

- This feature comes from Validity Insights which is sourced from authoritative data providers.
- This attribute indicates the date that the email domain was registered. Example: Gmail domain is dated to 2004.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing, or email domain is invalid Integer: The number of days since the email domain was created	**Behavior:** Submits a real email with an established domain such as Gmail, Outlook, etc. **Ekata data:** Often returns a domain creation date that is dated at least 5 years back from the current date.	**Behavior:** Prefers creating a new email domain or using a higher risk domain to fake being a legitimate business or to avoid having a history of use. **Ekata data:** Will often return a domain creation date that is dated very recently, within the last year.

Primary/Secondary Email Match to Name

Definition

- This attribute is derived from Validity Insights, which is sourced from authoritative data providers.
- This attribute checks the match status between the primary email and name, if both are provided in the API request.
- This attribute also validates by checking the input name against the name associated in Validity Insights email records to determine if there is a match.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email or name is missing, or email is invalid *match*: Name linked to email matches Input name; low risk *no-match*: Name linked to email was found but did not match Input name; high risk no-name-found: No name was found associated with email.	**Behavior:** Submits their real name and real email in signups. **Ekata data:** Often returns a match unless coverage is low.	**Behavior:** Prefers temporary or disposable emails that they change frequently. If they are impersonating a victim, they rarely use the victim's email unless they have gained full login access. **Ekata data:** In most scenarios there will not be a name associated with the email.

Primary/Secondary Email Match to Address

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute checks the match status between the email address and the input address.
    - Match: Entity location matches input location address line 1, address line 2, city, state, and postal code.
    - Postal match: Entity location postal code matches input location postal code.
    - Zip4-match: Entity location postal code zip+4 matches input location postal code zip+4.
    - City-state-match: Entity location city and state matches input location city and state.
    - Metro-match: Entity location is in the same metro area as input location.
    - Country-match: Entity location country matches input location country.
    - No match: Entity location does not match input location.

Assessing Risk

Field Values	Good Consumers	Fraudsters
Match: Low risk *Postal match or zip+4 match*: Medium risk *City-state-match* or *metro-match*: Medium risk Country match: High risk *No match*: Highest risk	**Behavior:** Submits their real email address and real address in transactions, usually without typos, and usually lives at the same address for a year or longer. **Ekata data:** Can often verify the match. May not be able to match due to coverage gaps, subletting, or minors under 18 years.	**Behavior:** Typically enters the victim's address but may falsify the email address (or vice versa). **Ekata data:** Will do the email to address match to assess and qualify the risk.

Primary/Secondary Email Registered Owner Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input email is missing or email is invalid String: The full name of the registered owner of the email address.	**Behavior:** Matches with the name entered **Ekata data:** Often returns a name unless coverage is low.	**Behavior:** Does not match with the input name.

IP is Valid

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, or on provider timeout *true*: The IP is a valid IP address or is in a private range *false*: The IP is not a valid IP address	**Behavior:** IP is valid and is not within a private range.	**Behavior:** IP is invalid or filled with masked data to obfuscate the true location.

IP Proxy Risk

Definition

- Assesses whether there is reason to believe this is a proxy IP address

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout	**Behavior:** Do not use a proxy	**Behavior:** Hide behind a VPN or proxy to appear they are located elsewhere.

IP Geolocation Postal Code

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout	**Behavior:** Matches up or is consistent with other location data provided.	**Behavior:** Is not consistent with other location data provided.

IP Geolocation City Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout	**Behavior:** Matches up or is consistent with other location data provided.	**Behavior:** Is not consistent with other location data provided.

IP Geolocation Subdivision

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout String: Contains a subregion of country which the IP is located in.	**Behavior:** Matches up or is consistent with other location data provided.	**Behavior:** Is not consistent with other location data provided.

IP Geolocation Country Name

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout	**Behavior:** Matches up or is consistent with other location data provided.	**Behavior:** Is not consistent with other location data provided.

IP Geolocation Country Code

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates the country location of the input IP address, returned as a two-character country abbreviation (e.g., US, CA, SG, DE, etc.).
- This attribute is derived from the latitude and longitude coordinates of the IP address to return the accompanying country.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout Otherwise, will return the ISO-3166 alpha-2 country code of the address. See: ISO-3166	**Behavior:** Uses their normal IP address associated with their country of residence **Ekata data:** Returns a country code that matches the country of residence if available	**Behavior:** Prefers proxy IPs or other ways to hide their identity or uses an IP in conjunction with mismatched identities **Ekata data:** May return a country code that does not match the country of the primary address, or originates from a country associated with higher incidences of fraud (Russian Federation, Algeria, etc.)

IP Geolocation Continent Code

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: When Input IP address is missing, is invalid, is in a private range, or on provider timeout Otherwise, will return two-letter continent code of the address.	**Behavior:** Matches up or is consistent with other location data provided.	**Behavior:** Is not consistent with other location data provided.

IP Match to Primary / Secondary Name [deprecated]

Definition

- This attribute comes from Validity Insights, which is sourced from authoritative data providers.
- This attribute indicates if the input name matches any of the people or businesses linked to the IP address

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Signal will return as null due to this signal being deprecated on April 2, 2024.	**Behavior:** Matches up or is consistent with names provided in other fields.	**Behavior:** Is not consistent with names provided in other fields.

IP Primary/Secondary Address Distance

Definition

- This attribute is derived from Validity Insights which is sourced from authoritative data providers.
- This attribute calculates the distance in miles between a given IP address's geolocation and physical address if both are provided. Both addresses need to be validated to at least the city level to get a response.
- The attribute is derived by measuring the latitude and longitude of both the IP address and the physical address and comparing the two to provide a distance calculation using Haversine formula distance in miles.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input IP or address is missing, or IP or address is invalid, or precision of IP location or address is less than city-level 0: Medium-low risk (IP geo-locations are usually only precise to the postal level, so a zero usually indicates a partial address was given, rather than the IP and address being the exact same location) 1-9: Low risk 10-99: Neutral risk 100+: High risk	**Behavior:** Typically shop from home, work, or on commute, and only rarely from a great distance from their home address. **Ekata data:** Generally, sees a small distance between IP location and primary/secondary address.	**Behavior:** Prefers proxy IPs or public Wi-Fi to hide their identity and includes addresses of cardholder victims which can come from anywhere in the world. For secondary addresses, tends to ship packages to vacant addresses, commercial mail drops, hotels, or other locations where they can pick up safely while not compromising their identity, and which may be far away from the IP location. **Ekata data:** Often sees a large distance between IP location and primary/secondary address.

IP Primary / Secondary Phone Distance

Definition

- This attribute is derived from Validity Insights which is sourced from authoritative data providers.
- This attribute calculates the distance in miles between the input IP address's geolocation and input phone location if both are provided.
- The attribute is derived by measuring the latitude and longitude of both the IP address and the phone location and comparing the two to provide a distance calculation using Haversine formula distance in miles.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: Input IP or phone is missing, or IP or phone is invalid 0: Medium-low risk (IP geo-locations are usually only precise to the postal level, so a zero usually indicates a partial address was given, rather than the IP and phone being the exact same location) 1-9: Low risk 10-99: Neutral risk 100+: High risk	**Behavior:** Typically shop from home, work, or on commute, and only rarely from a great distance from their phone's billing address except in the cases the phone is billed to a different address than the person resides. **Ekata data:** Generally, sees a small distance between IP location and phone location.	**Behavior:** Prefers proxy IPs or public Wi-Fi to hide their identity, and burner or temporary phones for which the associated location can vary. **Ekata data:** Often sees a large distance between IP location and phone location.

Identity Network Score

Definition

- Identity Network Score is a machine learning prediction that provides insight into how risky a digital interaction is based on activity patterns of the identity elements that are being used.
- Activity patterns that the Network Score focuses on include velocity, popularity, volatility, and age/maturity of the element(s).
    - Velocity: how often element(s) are used
    - Popularity: At how many merchants element(s) are used
    - Volatility: how often element(s) are used with other elements
    - Age/maturity: when elements were first/last seen
- To return a score, at least one valid element is needed. For best results, it is recommended sending as much of the following information as possible:
    - Name (primary or secondary)
    - Phone (primary or secondary)
    - Address (primary or secondary)
    - Email Address (primary or secondary)
    - IP Address

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: A service timeout is experienced or did not get enough Inputs Range: 0.000 - 1.000 <.33: Low risk .33-.8: Uncertain >.8: High risk **Note:** Risk thresholds will vary per customer as it depends on the customer's specific distribution.	Examples: • 3 IP addresses used with primary address in last 3 months • Primary address and email used together at 5 businesses in last month • Email seen in 0 transactions in last 24 hours • Phone and email first seen together 2 or more years ago	Examples: • 15 IP addresses used with same email in last 6 months • Primary address used in 28 digital interactions in 1 month • 20 primary addresses used with one secondary address in 3 months • Email seen in 15 more transactions in last 2 weeks vs. 3 months

Identity Risk Score

Definition

- The Identity Risk Score is a comprehensive risk score calculated in real time that combines authoritative data (match statuses, metadata, linkages) from Validity Insights as well as usage patterns of elements in the Interaction Insights.
- To return a score, the required Inputs must be provided. For best results, it is recommended sending as much of the following information as possible:
    - Name (primary or secondary)
    - Phone (primary or secondary)
    - Address (primary or secondary)
    - Email Address (primary or secondary)
    - IP Address

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: A service timeout is experienced Range: 0 - 500 <250: Low risk 250-350: Uncertain >350: High risk **Note:** Risk thresholds will vary per customer as it depends on customer's specific distribution.	Examples: ● Email, phone, and address are all valid and match to name ● IP is valid and risk is low ● Short distance between address and IP or phone ● Email and address first seen together 2 or more years ago ● Email first seen 2 or more years ago	Examples: ● Email, phone, and addresses are either not found or couldn't be validated ● IP geolocation does not match physical address ● Large distance between address and IP or phone ● 15 IP addresses used with same email in last 6 months ● Primary address used in 28 digital interactions in 1 month

Email Risk Score

Definition

- Email Risk Score assesses the risk level of an email address. The score is derived from a model that leverages insights from the Identity Network including email tumbling detection, email linkages to other PII inputs and disposable email domain list service.
- To return a score, an email address must be provided. For best results, it is recommended sending at least one of the following as well for geolocation purposes:
    - Phone (primary or secondary)
    - Address (primary or secondary)
    - IP Address

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: A service timeout is experienced Range: 0.000 – 1.000 <0.3 Low Risk 0.31 - 0.5 Neutral Risk 0.51 - 0.8: Medium Risk 0.8-0.97: High risk >0.97: Very high risk **Note:** Risk thresholds will vary per customer and country as it depends on customer's specific risk tolerance and regional behavior. This is why providing phone, address, or IP address is important for geolocation purposes.	Examples: • Mailbox velocity is low • Email domain is not disposable • Email first seen 2 or more years ago	Examples: • Mailbox velocity is high • Email first seen today • Email domain is disposable

Primary Email Mailbox Velocity

Definition

- An integer value for the velocity (frequency) a mailbox has been seen in the past 180 days.
- A mailbox is the un-tumbled name part of an email address. For example: johndoe@gmail.com, john.doe@gmail.com, and johndoe+123abc@gmail.com all resolve to the same mailbox.

Assessing Risk

Field Values	Good Consumers	Fraudsters
null: The mailbox has not been seen in 180 days, or a service timeout has been experienced Range: 1 – Infinity null: Neutral Risk 1 – 5: Low Risk 5 – 10: Neutral Risk 11 – 20: Medium Risk 21 – 100: High risk >100: Very high risk **Note:** Risk thresholds will vary per customer and country as it depends on customer's specific risk tolerance and regional behavior. This is why providing phone, address, or IP address is important for geolocation purposes.	**Behavior:** Typically, they will have a mailbox velocity (mailbox was seen) of less than 10 times in the past 180 days.	**Behavior:** Typically, will have a mailbox velocity (mailbox was seen) of more than 20 times in the past 180 days.

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.