Identity Insights for Transactions Data Dictionary

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

Reinitiation & Assessing Risk

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 the Mastercard Identity Network as well as usage patterns of elements in the Mastercard Identity Network.

To return a score, the required Inputs must be provided. For best results, it is recommended to send as much of the following information as possible.

Reason Code: The reason code represents the highest-level explanation of the Identity Risk Score, categorized by the inputs that were most important to determine overall riskiness. Each transaction will receive only one reason code associated with the score.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: when we experience a service timeout *Range: 0 - 500* *<250: low risk* *251-350: uncertain* *>351: 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+ years ago* *Email first seen 2+ 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*

Full list of possible reason codes:

High Severity Reason Codes

AA - Consumer Identity is suspicious

AB - Increased Risk associated with Email

AC - Increased Risk associated with Email & IP

AD - Increased Risk associated with Email & Address

AE - Increased Risk associated with Email & Phone

AF - Increased Risk associated with Email & Name

AG - Increased Risk associated with IP

AH - Increased Risk associated with IP & Phone

AI - Increased Risk associated with IP & Address

AJ - Increased Risk associated with IP & Name

AK - Increased Risk associated with Address

AL - Increased Risk associated with Address & Phone

AM - Increased Risk associated with Address & Name

AN - Increased Risk associated with Name

AO - Increased Risk associated with Name & Phone

AP - Increased Risk associated with Phone

AQ – Increased Risk associated with Device & Email

AR - Increased Risk associated with Device & IP

AS - Increased Risk associated with Address & Device

AT - Increased Risk associated with Device & Name

AU - Increased Risk associated with Device & Phone

Medium Severity Reason Codes

JA - New Consumer or not sufficient information

JB - Medium Risk Signals associated with Email

JC - Medium Risk Signals associated with Address

JD - Medium Risk Signals associated with Phone

JE - Medium Risk Signals associated with Name

JF - Medium Risk Signals associated with IP

Low Severity Reason Codes

RA - Consumer Trust Established across all elements

RB - Established Credibility for Email

RC - Established Credibility for Email & IP

RD - Established Credibility for Email & Address

RE - Established Credibility for Email & Phone

RF - Established Credibility for Email & Name

RG - Established Credibility for IP

RH - Established Credibility for IP & Phone

RI - Established Credibility for IP & Address

RJ - Established Credibility for IP & Name

RK - Established Credibility for Address

RL - Established Credibility for Address & Phone

RM - Established Credibility for Address & Name

RN - Established Credibility for Name

RO - Established Credibility for Name & Phone

RP - Established Credibility for Phone

RQ - Established Credibility for Device & Email

RR - Established Credibility for Device & IP

RS - Established Credibility for Address & Device

TY - Established Credibility for Device & Name

RU - Established Credibility for Device & Phone

Billing Address Validity Level

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates the level to which the physical address could be validated. For example, if the address was only valid to the city level (but not to 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 *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* *Valid: Neutral 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.* *Typos are relatively frequent.* ***Mastercard data:** Most common validates the full address provided.* *It may identify it as invalid or partially valid.*	***Behavior:** 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 of the victim. If they do not have the full address, they may fabricate an address that includes the details they do have.* ***Mastercard data:** May validate the address but may identify it as invalid or partially valid.*

Billing Address Match to Name

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates if the input name matches any of the people linked to the physical address.

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* *Not found: No name associated with address found; neutral risk, high risk where coverage is high*	***Behavior:*** *Submits their real name and real address in account sign ups, usually without typos, and usually lives at the same address for a year or longer.* ***Mastercard data:*** *Can often verify the match. May be able to match due to coverage gaps, subletting or minors under 18 years.*	***Behavior:*** *Typically enters the victim'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.* ***Mastercard data:*** *Sometimes verifies the match, but often will return no-match or no name found.*

Billing Address First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the first time that the inputted billing address has been seen in Mastercard's network.

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 provided or is not validated to at least street level *0: Never been seen before; High risk* *1-7: High-Medium risk* *7+: Slightly lower risk*	***Behavior:** Submits their real billing address, which is typically used online frequently, by themselves, other current and previous occupants* ***Mastercard data:** It is uncommon that the address has not been seen before, although this varies country-to-country. In lower coverage countries, there may be a higher prevalence of never seen addresses. Most commonly the address was first seen over a year ago.*	***Behavior:** Billing addresses generally belong to the card holder victim, who may or may not shop online regularly.* ***Mastercard data:** It is still rare that the address has not been seen before, but never seen or only recently seen addresses are much more common among fraudulent transactions*

Billing Address Last Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the last time that the input billing address has been seen in Mastercard's network.

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 provided or is not validated to at least street level *0: Never been seen before; High risk* *1-7: High -Medium risk* *7+: Slightly lower risk*	***Behavior:** Submits their real billing address, which is typically used online frequently, by themselves, other current and previous occupants* ***Mastercard data:** It is uncommon that the address has not been seen before, although this varies country-to-country. In lower coverage countries, there may be a higher prevalence of never seen addresses. Frequencies between a week and a month are most common.*	***Behavior:** Billing addresses generally belong to the card holder victim, who may or may not shop online regularly.* ***Mastercard data:** It is still rare that the address has not been seen before, but never seen or recently seen addresses are much more common among fraudulent transactions*

Billing Shipping Address Relationship

Definition

This attribute is derived from the Identity Network is sourced from Mastercard's global customers.

This attribute provides the relationship in the Identity Network between the provided billing and shipping addresses, if both are provided.

Both addresses need to be validated to at least the city level to get a response.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
null: Where the address is not provided or is not validated to at least street level *match: Very Low risk* *city_match; Low risk* *seen_together; Medium risk* *seen_with_others; High risk* *no_relationship; High Risk*	***Behavior:*** *Typically continuously ship to the same addresses* ***Mastercard Data:*** *an established history between the billing and shipping address correlates to a lower likelihood of fraud.*	***Behavior:*** *Use their victim's billing addresses but ship to a convenient address within the location they are committing the fraud.* ***Mastercard Data:*** *The lack of history between two addresses correlates to a greater risk of fraud*

Device Risk Score

Definition

Evaluates the relationship between the device elements alongside historical IP and device risk across the device network to determine riskiness. Output between 0.000-1.000

To return a score, the required Inputs must all be provided.

IP Address	Screen Width
User Agent	Language
Screen Height	Time Zone

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: invalid or missing inputs *Range: 0 – 1* *<0.6: Low Risk* *0.6 - 0.9: Neutral Risk* *>=0.9: High Risk*	***Behavior:*** *Uses their normal device(s) that they've owned for across all the various places they interact online.* ***Mastercard Data:*** *Identifies the device as low risk based on device characteristics matching historical network patterns for good behaviors and there is no device attribute abnormality.*	***Behavior:*** *spoof or manipulate device or to use techniques to mask device or IP address.* ***Mastercard Data:*** *Often identifies the device as risky based on device attributes and behavioral patterns associated with a fraudulent account.*

Device Type

Definition

The type of device the end user is using for this request.

This information is derived from the user agent and is available whenever a recognized User Agent (UA) string is passed in the request.

This signal is primarily used as metadata but may be valuable in identifying anomalies within your business based off volume/geographic trends of device types

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Varies based on the device being used in the transaction. *null: The device type cannot be determined*	***Behavior:** Uses a device type that aligns with the platform / application / browser being used and is appropriate to the use-case being served or which is commonly found in the region that the request originates from.*	***Behavior:** May use an emulator to spoof device inputs leading to inconsistencies with the application being used and the typical device prevalence within that region*

Device Platform

Definition

The type of operating system Installed on the device that the end user is using for this request.

This information is derived from the user agent and is available whenever a recognized User Agent (UA) string is passed in the request.

This signal is primarily used as metadata but may be valuable in identifying anomalies within your business based off volume/geographic trends of device types

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Varies based on the device being used in the transaction. *null: The operating system cannot be determined*	***Behavior:*** *Uses an operating system that aligns with the device type / application / browser being used and is appropriate to the use-case being served*	***Behavior:*** *May use an emulator to spoof device inputs leading to inconsistencies with the application being used and the typical operating system prevalence within that region*

Device Browser

Definition

This attribute comes from the user-agent value collected from the device by the customer.

This attribute indicates the type of application that is used in the transaction, which maybe inappropriate for the use case being executed by the customer (E.g. a mobile browser being returned for a food delivery app).

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Varies based on the device being used in the transaction. *null: The operating system cannot be determined*	***Behavior:** Uses an application that aligns with the application / browser flow being used and is appropriate to the use-case being served*	***Behavior:** Can exploit third party applications to commit fraud*

Device Browser IP Time Zone Difference

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

The difference in minutes between the browser's time zone and the IP address's time zone.

For this signal to be generated both the IP Address and the Device Time-zone need to be provided.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Invalid inputs *0 – Low Risk* *1 - Medium Risk* *2+ – High Risk - Potential VPN usage or geo location spoofing*	***Behavior:*** *keeps browser's time zone or IP address as is, without masking or tempering.* ***Mastercard data:*** *There is no difference between the two time zones. The value is 0.*	**Behavior***: purposely changes either or both the browser's time zone and IP address time zone to hide user's location.* ***Mastercard data:*** *Risk level increases when the value is not 0. Potential indication of location spoofing or VPN usage by the end users.*

Device IP - First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

The count of days since a Device and IP address were initially observed.

For this signal to be generated all of the following inputs need to be provided: IP Address, User-Agent, Time-zone, Language, Screen Height, Screen Width

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: invalid or no inputs *0 – 1 Days – High Risk* *7 – 60 Days – Medium Risk* *> 60 days. - Lower Risk* *The higher the count of days, the lower the risk.*	***Behavior:*** *uses their own device and IP without any manipulation or masking.* ***Mastercard data:*** likely has a large value since we have seen this combination a long time ago.	***Behavior:*** manipulates device attributes or uses a virtual machine to mask their device and IP address. ***Mastercard data:*** recently seen combinations have much higher association with fraud.

Device IP Payment - First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

The count of days since a Device, a Payment Credential and IP Address were initially observed.

For this signal to be generated all of the following inputs need to be provided: IP Address, User-Agent, Time-zone, Language, Screen Height, Screen Width. Payment Account Number

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: invalid or no inputs *0 – 1 Days – High Risk* *7 – 60 Days – Medium Risk* *> 60 days. - Lower Risk* *The higher the count of days, the lower the risk.*	***Behavior:*** *Uses their own payment credential, device and IP without any manipulation or masking.* ***Mastercard data:*** *likely has a large value since we have seen this combination a long time ago.*	***Behavior:*** *acquires a payment credential online and manipulates device attributes or uses a virtual machine to masks their device and IP address.* ***Mastercard data:*** *recently seen combinations have much higher association with fraud.*

Device IP Email – First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

The count of days since a Device, an Email and IP address were initially observed.

For this signal to be generated all of the following inputs need to be provided: IP Address, User-Agent, Time-zone, Language, Screen Height, Screen Width, Email Address

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: invalid or no inputs *0 – 1 Days – High Risk* *7 – 60 Days – Medium Risk* *> 60 days. - Lower Risk* *The higher the count of days, the lower the risk.*	***Behavior:** Submits their real email address and uses their own device without any manipulation or masking of IP.* ***Mastercard data:** likely has a large value since we have seen this combination a long time ago.*	***Behavior:** uses a disposable email, manipulates device attributes or uses a virtual machine to masks their device and IP address.* ***Mastercard data:** recently seen combinations have much higher association with fraud.*

Device Email Payment - First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

The count of days since a Device, an Email and Payment Credential were initially observed.

For this signal to be generated all of the following inputs need to be provided: User-Agent, Time-zone, Language, Screen Height, Screen Width, Email Address, Payment Account Number

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: invalid or no inputs *0 – 1 Days – High Risk* *7 – 60 Days – Medium Risk* *> 60 days. - Lower Risk* *The higher the count of days, the lower the risk.*	***Behavior:** Submits their real email address and uses their own device and payment credential.* ***Mastercard data:** likely has a large value since we have seen this combination a long time ago.*	***Behavior:** acquires a payment credential online, uses a disposable email address and manipulates device attributes or uses a virtual machine to masks their device* ***Mastercard data:** recently seen combinations have much higher association with fraud.*

Email Risk Score

Definition

This attribute helps to identify the overall risk of an email address. The attribute considers metadata sourced by Identity Network, e.g., whether the email is tumbled or not, the age of the domain, and behavioral characteristics sourced by Identity Network for the email address.

Assessing Risk

Field Values	*Low Risk*	*High Risk*
Null: Input email is missing or invalid *<0.6: Low Risk* *0.6 - 0.9: Neutral Risk* *>=0.9: High Risk*	***Behavior:*** *Uses their normal email address that they've had for many years across all the various places they interact online.* ***Mastercard Data:*** *Identifies the email address as low risk based on email attributes and behavioral patterns that match normal good behaviors among the network if available.*	***Behavior:*** *Prefers disposable emails newly created emails, or tumbled emails to obfuscate their identity when creating a fraudulent account.* ***Mastercard Data:*** *Often identifies the email address as risky based on email attributes and behavioral patterns associated with a fraudulent account.*

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	*Low Risk*	*High Risk*
Null: Input email is missing or invalid *True: High Risk* *False: Low Risk*	***Behavior:*** *Submits their real email address, which is a normal working static email.* ***Mastercard Data:*** *Identifies the email as disposable or not, if available in Mastercard network.*	***Behavior:*** *Prefers to use disposable emails rather than their legitimate emails to mask their identity.* ***Mastercard Data:*** *Emails may be identified as disposable.*

Email Valid

Definition

This attribute returns a true/false response that signals whether the email supplied is a valid email address or not.

This attribute is from our Mastercard Identity Network, 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* ***Mastercard data:*** *Identifies the email as valid if available in Mastercard's Network.*	***Behavior:*** *Prefers temporary or newly created emails or may enter a fake email if they do not expect it to be verified.* ***Mastercard data:*** *Emails may be identified as valid*

Email First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the first time that the input email has been seen in Mastercard's network.

The email address does not need to be active for it to be in Mastercard's network.

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.* ***Mastercard data:*** *Genuine emails were likely first seen the 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.* ***Mastercard data:*** *Likely have never seen the email before or have seen it only recently. Emails first seen a long time ago are unlikely.*

Email Last Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the last time that the input email has been seen in Mastercard's network.

The email address does not need to be active for it to be in Mastercard's network.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input email is missing, or email is invalid *0: Never seen before, high risk* *1-7: High risk* *8-30: Low risk* *31-365: Medium risk* *366+: High risk*	***Behavior:*** *Typical behavior for online buyer interactions happens once or a few times a month. Daily interactions are less common.* ***Mastercard data****: Frequencies between a week and a month are most common.*	***Behavior:*** *Fraudsters may use stolen data or create disposable emails associated with a higher frequency and velocity of online behavior.* ***Mastercard data:*** *Has not seen the email in the past 12 months, which may indicate a stolen identity. Or the email has daily frequencies of interactions which may indicate fraudulent online behavior.*

Email Domain Creation Date

Definition

This feature comes from the Mastercard Identity Network 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	***Behavior:*** *Submits a real email with an established domain such as Gmail, Outlook, etc.*	***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.*
Timestamped date, e.g., 2004-08-26	***Mastercard data:*** *Often returns a domain creation date that is dated at least 5 years back from current date.*	***Mastercard data:*** *Will often return a domain creation date that is dated very recently, within the last year.*

Email Match to Name

Definition

This attribute is derived from the Mastercard Identity Network, 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 provided name against the name associated in Mastercard Identity Network 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* *Not found: No name was found associated with email*	***Behavior**: Submits their real name and real email in signups.* ***Mastercard data:** Often returns a match unless coverage is low.*	***Behavior:** Prefers temporary or disposable emails that change frequently. If they are impersonating a victim, they rarely use the victim's email unless they have gained full login access.* ***Mastercard data:** In most scenarios there will not be a name associated with the email.*

IP Risk Score

Definition

This attribute helps identify the overall risk of an IP. The attribute considers metadata sourced by Mastercard's Identity Network, e.g., IP is associated with a VPN, the relative risk that the VPN carries, and behavioral characteristics sourced by Mastercard's Identity Network for the associated VPN and the IP address.

The Score allows for greater control & flexibility. Results are determined by the risk tolerance threshold defined and set by the customer.

Leveraging the Score is determined on the approach of risk assessment implemented. The score perform well in machine learning models and rules-based engines.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input IP is missing, or IP is invalid *Score* *<0.6: Low risk* *0.6-0.9: Neutral risk* *>0.9: High risk*	***Behavior:*** *Uses their normal IP address on their laptop, mobile phone, desktop, or other device, from the various places they shop.* ***Mastercard data:*** *Identifies the IP address as low risk based on IP attributes and behavioral patterns that match normal good transactions if available.*	***Behavior:*** *Prefers proxy IPs, public Wi-Fi, and other methods to hide their identity, and behave in different ways, e.g., submitting several transactions across different merchants in quick succession.* ***Mastercard data:*** *Often identifies the IP address as risky based on IP attributes and behavioral patterns that are associated with fraudulent transactions.*

IP Proxy Detection

Definition

This attribute helps identify if there is a proxy being used to mask the identification of an IP address. The attribute is derived from metadata sourced by Mastercard's Identity Network and global source providers.

A flag indicating whether the IP is suspected to be a proxy based on Mastercard's Identity Network's detection of IP proxies. Boolean (nullable)

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
TRUE : A proxy is suspected *FALSE: A proxy is not suspected*	***Behavior:*** *Uses their normal IP address on their laptop, mobile phone, desktop, or other device, from the various places they shop.* *Some privacy conscious customers may also use VPNs.* ***Mastercard data:*** *In general transactions from assigned IPs are less likely to be fraudulent*	***Behavior:*** *Prefers the use of proxy IPs, public Wi-Fi, and other methods to hide their identity, and behavior e.g., submitting several transactions across different merchants in quick succession.* ***Mastercard data:*** *Indicates an increased likelihood of fraud when VPNs are used, though as VPN usage becomes more main stream this trend is becoming less pronounced.*

IP Proxy Risk Class

Definition

The attribute is derived from metadata sourced by Mastercard's Identity Network and global source providers.

This attribute helps identify whether the proxy in use is considered low, medium or high risk based on its proxy classification.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Low Risk: OS provider or Corporate VPN *Medium Risk: Hosted VPN or Web Browser* *High Risk: Confirmed TOR node or Hosted VPN IP with TOR like behavior patterns*	***Behavior:*** *may use corporate VPNs or OS provided VPNs* ***Mastercard data:*** *Indicates that VPN usage is becoming more prevalent and as a result diluting the risk which would typically be associated to medium and low risk VPNs*	***Behavior:*** *may use IPs associated to TOR to facilitate attacks or be using alternate proxies at high frequencies* ***Mastercard data:*** *Often identifies that requests originating from high risk IP proxy group have an increased risk of potential fraud.*

IP Last Seen Days

Definition

This attribute indicates when the last time the input IP address has been seen in Mastercard's network.

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input IP is missing, or IP is invalid *0: Never seen before; High risk* *1-7: High risk* *8-89: Neutral risk* *90+: Low risk*	***Behavior:*** *Most online buyers only shop once per month or less. Few shop weekly, and very few shop daily. Also, there are many more IP addresses than there are consumers, so while some shoppers may share an IP if they are using public Wi-Fi for example, the typical pattern is that each IP represents a portion of one shopper's transactions.* ***Mastercard data:*** *Most IP addresses don't show up more than once per week in the Mastercard Network. The frequency around one month is the most common. Daily frequencies are rare.*	***Behavior:*** *Fraudsters often hide their identity using proxy IPs, or using public Wi-Fi. This tends to cluster fraudulent transactions among a smaller set of IPs. Also, fraudsters generally want to take advantage of their stolen credit card data before the card gets canceled, and so make frequent purchases with it.* ***Mastercard data:*** *IPs show up relatively frequently in our Network. A fraudulent transaction often has an IP seen in the last day, or in the last few days. It would be rare for the IP to not have been seen for months.*

IP Connection Type

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates the connection type of the input IP address, returns one of following values: cable-DSL, corporate, cellular, or dialup

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 *cable-dsl: Low risk* *corporate: Medium risk* *cellular: Neutral risk* *dialup: Neutral risk*	***Behavior:** Uses their normal IP address in online interactions, typically from their residential home, or from their mobile device.*	***Behavior:** Prefers proxy IPs or other ways to hide their real identity.*

IP Provider Country Code

Definition

This attribute comes from the Mastercard Identity Network, 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 a two-character country code for the country which the IP provider is located in*	***Behavior:** Uses their normal IP address associated with their country of residence*	***Behavior:** Is not consistent with other location data provided.*

IP Provider State

Definition

This attribute comes from the Mastercard Identity Network, 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 provider is located in*	***Behavior:** Uses their normal IP address associated with their country of residence*	***Behavior:** Is not consistent with other location data provided.*

IP Provider City

Definition

This attribute comes from the Mastercard Identity Network, 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 city which the IP provider is located in*	***Behavior:*** *Uses their normal IP address associated with their country of residence*	***Behavior:*** *Is not consistent with other location data provided.*

IP Provider Carrier

Definition

The name of internet service provider (ISP) used by the customer's device while connecting to your service, which is sourced from authoritative data providers.

IP carrier name will be for Proxy or VPN provider if users are using such services for connecting with your application

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 the name of the provider of the IP being used in the request*	***Behavior:*** *Use an IP Address from an established IP provider*	***Behavior:*** *Use IP Address from Proxy or VPN providers*

IP Billing Address Distance

Definition

This attribute is derived from the Mastercard Identity Network which is sourced from authoritative data providers.

This attribute calculates the distance in miles between the input IP address's geolocation and input billing 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 billing 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 billing address is missing, or IP or billing address is invalid, or precision of IP location or billing 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 billing address was given, rather than the IP and address being the exact same location)* *1-199: Low risk* *200-499: Medium risk* *500-999: High-Medium Risk* *1000+: High risk*	***Behavior:** Typically use an IP provider located based in the country they are operating from* ***Mastercard data:** Generally, sees a small distance between IP location and billing address.*	***Behavior:** Prefers proxy IPs or public Wi-Fi to hide their identity and includes billing addresses of cardholder victims which can come from anywhere in the world.* ***Mastercard data:** Often sees a large distance between IP location and billing address.*

IP Shipping Address Distance

Definition

This attribute is derived from the Mastercard Identity Network which is sourced from authoritative data providers.

This attribute calculates the distance in miles between the input IP address's geolocation and input shipping 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 shipping 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 shipping address is missing, or IP or shipping address is invalid, or precision of IP location or shipping 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 shipping address was given, rather than the IP and shipping address being the exact same location)* *1-199: Low risk* *200-499: Medium risk* *500-999: High-Medium Risk* *1000+: High risk*	***Behavior:** Typically use an IP provider located based in the country they are operating from and ship to a location which is also in relatively close proximity* ***Mastercard data:** Generally, sees a small distance between IP location and shipping address.*	***Behavior:** Prefers proxy IPs or public Wi-Fi to hide their identity which can come from anywhere in the world. For shipping addresses, they tend 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.* ***Mastercard data:** Often sees a large distance between IP location and address.*

Merchant Category Ratio

Definition

This attribute comes from the Identity Network, which is sourced from Identity Services global customers.

This attribute is a ratio of the purchase amount compared to the median purchase amount seen for other similar merchants in the same category.

The higher the ratio means that the purchase amount is further from the median purchase amount observed.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input purchase amount or merchant category code is missing *0-09.: Neutral risk* *1.0-2.0: Medium high risk* *2.0+: Medium high risk*	***Behavior:** makes online transactions that are reasonable and considered normal amongst other normal users. Occasionally bigger or smaller than average purchases may occur, but not the norm.* ***Mastercard Data**: may return a ratio closer to 1 to represent normal transaction behavior*	***Behavior:** will try to make abnormally large purchases in rapid succession using stolen credentials to maximize their gains as much as possible or will make a bunch of smaller than average purchases to fly under the radar.* ***Mastercard Data:** may return a much smaller or much higher ratio, more commonly a much higher ratio, like 2+.*

Payment Cardholder Name First Seen Days

Definition

This attribute comes from the Identity Network, which is sourced from Identity Services global customers.

This attribute indicates the first time the payment account number and cardholder name have been seen together in the Identity Network.

Both the payment card (account number in the request payload) and cardholder name need to be inputted to be returned a non-null response

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input cardholder name or payment account number is missing *0: Never seen before, neutral risk* *1-7: High risk* *8+: Medium low risk*	***Behavior:*** *uses their real credit/debit card that is in their own name and follows a regular transaction frequency pattern (e.g. weekly or monthly). For most consumers, cards are well established of 1+ years, but occasionally they may open a new account that would have <1 year of transaction history.* ***Mastercard Data:*** *In scenarios where there is low coverage, a low value (<7) may be returned. Otherwise, 7+ should be expected for cardholders who have established some transaction history with their card.*	***Behavior:*** *uses stolen credentials, or opens a new line of credit using synthetic or real identity elements. Transactions are made in frequent volumes, cycling through multiple cards and/or identity elements.* ***Mastercard Data:*** *For fraudsters cycling through stolen credentials, we may see a valid response returned (i.e. 7+ days) for stolen credentials, but a lower number for new lines of credit opened using victim's identities*

Payment Cardholder Velocity

Definition

This attribute comes from the Identity Network, which is sourced from Identity Services global customers.

This attribute indicates the count of times the payment card and cardholder name have been observed in the network over the past 90 days.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input cardholder name or payment card is missing *0: They have not been observed together in last 90 days; neutral risk* *1-5: Low risk* *6-10: Neutral risk* *10-15: Medium high risk* *16+: Very high*	***Behavior:*** *Typically, only transact a few times a month or weekly, and sometimes even less frequently if the cardholder possesses multiple accounts.* ***Mastercard Data:*** *may return a lower velocity count (0-10) in line with average consumer spending.*	***Behavior:*** *Using stolen credentials, fraudsters may attempt to make many transaction attempts far beyond the average consumer across multiple merchants to increase their chances of success.* ***Mastercard Data:*** *may return a very high velocity count (15+).*

Phone Valid

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute returns a true/false response that signals if the input phone number 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.* ***Mastercard 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.* ***Mastercard data:*** *May identify phone number as invalid.*

Phone Line Type

Definition

This attribute comes from the Mastercard Identity Network, 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: landline, fixed-VoIP, mobile, voicemail, toll-free, premium, non-fixed-VoIP, other.

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.* ***Mastercard 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.* ***Mastercard data:*** *Phone line types associated with higher risk will be identified, e.g., Non-fixed VoIP, landline, or other non-mobile line types.*

Phone Carrier

Definition

This attribute comes from the Mastercard Identity Network, 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.* ***Mastercard 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.* ***Mastercard data:*** *Often returns the name of a known phone carrier. However, carriers associated with prepaid, or VoIP services occur more frequently.*

Phone Match to Name

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates if the name associated with the input phone number matches the input name.

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* *Not 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.* ***Mastercard 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 they may use the victim's phone number if they don't expect it to be called or texted.* ***Mastercard data:*** *Will very rarely verify the match, and often will have no name attached to the phone.*

Shipping Address Validity Level

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates the level to which the physical address could be validated. For example, if the address was only valid to the city level (but not to 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 *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* *Valid: Neutral 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.* *Typos are relatively frequent.* ***Mastercard data:*** *Most common validates the full address provided.* *It may identify it as invalid or partially valid.*	***Behavior:*** *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 of the victim. If they do not have the full address, they may fabricate an address that includes the details they do have.* ***Mastercard data:*** *May validate the address but may identify it as invalid or partially valid.*

Shipping Address Match to Name

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from authoritative data providers.

This attribute indicates if the input name matches any of the people linked to the physical shipping address.

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* *Not found: No name associated with address found; neutral risk, high risk where coverage is high*	***Behavior:** Submits their real name and real address in account sign ups, usually without typos, and usually lives at the same address for a year or longer.* ***Mastercard data:** Can often verify the match. May be able to match due to coverage gaps, subletting or minors under 18 years.*	***Behavior:** Typically ship packages to vacant addresses, commercial mail drops, hotels, or other locations where they can pick up safely. These addresses will have no established relationship with the cardholder's name.* ***Mastercard data:** Sometimes verifies the match, but often will return no-match or no name found.*

Shipping Address First Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the first time that the inputted shipping address has been seen in Mastercard's network.

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 provided or is not validated to at least street level *0: Never been seen before; Neutral risk* *1-7: High risk* *7+: Slightly lower risk*	***Behavior:** Submits their real shipping address, which is typically used online frequently, by themselves, other current and previous occupants* ***Mastercard data:** It is uncommon that the address has not been seen before, although this varies country-to-country. In lower coverage countries, there may be a higher prevalence of never seen addresses. Most commonly the address was first seen over a year ago.*	***Behavior:** Shipping addresses generally belong to the perpetrator of the fraud, they tend to ship packages to vacant addresses, commercial mail drops, hotels, or other locations where they can pick up safely while not compromising their identity* ***Mastercard data:** It is still rare that the address has not been seen before, but never seen or only recently seen addresses are much more common among fraudulent transactions*

Shipping Address Last Seen Days

Definition

This attribute comes from the Mastercard Identity Network, which is sourced from Mastercard's global customers.

This attribute indicates the last time that the shipping address has been seen in Mastercard's network.

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 provided or is not validated to at least street level *0: Never been seen before; Neutral risk* *1-7: High risk* *7+: Slightly lower risk*	***Behavior:** Submits their real shipping address, which is typically used online frequently, by themselves, other current and previous occupants* ***Mastercard data:** It is uncommon that the address has not been seen before, although this varies country-to-country. In lower coverage countries, there may be a higher prevalence of never seen addresses. Frequencies between a week and a month are most common.*	***Behavior:** Shipping addresses generally belong to the perpetrator of the fraud, they tend to ship packages to vacant addresses, commercial mail drops, hotels, or other locations where they can pick up safely while not compromising their identity* ***Mastercard data:** It is still rare that the address has not been seen before, but never seen or recently seen addresses are much more common among fraudulent transactions*

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.