Identity for Accounts Data Dictionary

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

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	***Behavior:*** *Uses their normal email address that they've had for many years across all the*	***Behavior:*** *Prefers disposable emails newly created emails, or tumbled*

<0.6: Low Risk *0.6 - 0.9: Neutral Risk* *>=0.9: High Risk*	*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.*	*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	***Behavior:** Submits their real email address, which is a normal working email*	***Behavior:** Prefers temporary or newly created emails or may enter a fake email if they do not expect it to be verified.*

True: Neutral risk *False: High risk*	***Mastercard data:** Identifies the email as valid if available in Mastercard's Network.*	***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:** Likely I 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.* ***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 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 *Timestamped date, e.g.,*	***Behavior:** Submits a real email with an established domain such as Gmail, Outlook, etc.* ***Mastercard data:** Often returns a*	***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.*

2004-08-26	*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 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, e.g., IP is associated with a VPN, and behavioral characteristics sourced by Mastercard's Identity Network for the associated VPN and the IP address.

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 detected *FALSE: A proxy is not detected*	***Behavior:** Uses their normal IP address on their laptop, mobile phone, desktop, or other device, from the various places they shop.* *Most will use their normal IP address, but privacy conscious customers may also use VPNs* ***Mastercard data:** Identifies the IP address as low risk based on IP attributes and behavioral patterns that match normal good transactions if available.*	***Behavior:** Fraudsters commonly route traffic through proxy IPs, VPNs to hide their true origin. They often choose proxies with locations that match or are close to the billing address, shipping address of the user they are impersonating — making their activity look geographically consistent with the stolen identity* ***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 : OS provider or Corporate VPN *Medium: Hosted VPN or Web Browser* *High: Confirmed TOR node or Hosted VPN IP with TOR like behavior patterns*	***Behavior:*** *Good consumers more and more are using "good" proxies (e.g., Apple or Google's privacy proxy services, corporate VPNs) to protect their privacy.* ***Mastercard data:*** *Identifies the IP Proxy as low risk based on IP attributes and behavioral patterns that match normal good transactions if available.*	***Behavior:*** *Prefers proxy IPs from a lesser-known proxy group or known proxy groups often associated with fraudsters (e.g., TOR exit or relay).* ***Mastercard data:*** *Often identifies the IP proxy group as risky based on IP attributes and behavioral patterns that are associated with this group type.*

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*	***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*	***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*

1-7: High risk *8-89: Neutral risk* *90+: Low risk*	*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.*	*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 Geolocation 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*	***Behavior:** Uses their normal IP address associated with their country of residence* ***Mastercard 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* ***Mastercard data:** May return a country code that does not match country of primary address, or originates from a country associated with higher incidences of fraud (Russian Federation, Algeria, etc.)*

IP Geolocation Subdivision

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 is located in*	***Behavior:** Matches up or is consistent with other location data provided.*	***Behavior:** Is not consistent with other location data provided.*

IP Phone 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 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*	***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.* ***Mastercard 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.* ***Mastercard data:** Often sees a large distance between IP location and phone location.*

100+: High risk		

IP 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 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.* ***Mastercard data:** Generally, sees a small distance between IP location and 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 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.*

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 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 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 to 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* ***Mastercard data:** Returns a country code that matches the country of residence if*	***Behavior:** Prefers proxy IPs or other ways to hide their identity or uses a phone number in conjunction with mismatched stolen identities.* ***Mastercard 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*

	available	*(Russian Federation, Algeria, etc.)*

Phone Last Seen Days

Definition

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

This attribute indicated the last time the input phone number has been seen in Mastercard's network.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Input phone is missing or invalid *0: Never seen before; High risk* *1-7: High risk* *8-89: Neutral risk* *90+: Low risk*	***Behavior:*** *Most online buyers only shop or sign up to accounts once per month or less. Few shop weekly and very few shop daily. Typically, the same personal phone is used on all transactions. Multiple people typically do not share the same phone.* ***Mastercard data:*** *Most phones 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 uncommon.*	***Behavior:*** *Burner or throwaway phones are preferred which are used frequently.* ***Mastercard data:*** *Fraudulent signup often has a phone seen in the last day, or in the last few days.*

Phone 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 phone and email has been seen in Mastercard's network.

Assessing Risk

Field Values	*Good Consumers*	*Fraudsters*
Null: Both phone or email is missing or invalid. *0: Never seen together before, medium-high risk* *1-7: high risk* *7-179: medium-low risk*	***Behavior:*** *Submits their real email address and phone number, both of which are typically used online frequently. However, they are not always used together. Many accounts do not require both.* ***Mastercard data:*** *Likely first saw the phone or email a long time ago. Emails or phone numbers seen only recently*	***Behavior:*** *Typically utilizes disposable or temporary emails and change email addresses and phone numbers frequently. If they are impersonating a victim, they rarely use the victim's email unless they have gained full login access. 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.*

180+: very low risk	*are less common, since consumers do not change emails or phone numbers often.*	***Mastercard data:** Likely have never seen the email and phone used before or have seen them only recently. Email/phone pairs first seen a long time ago are unlikely.*

Phone 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.*

Phone to Address

Definition

This attribute comes from the Mastercard Identity Network, 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.* ***Mastercard 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.* ***Mastercard data:** Will do the phone to address match to assess and qualify the risk.*

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:*	***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*

Neutral risk *Valid_to_house_number_missing_apt: Neutral risk* *Valid: Neutral risk*		*partially valid.*

Address 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.*

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 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* *Note: risk thresholds will vary per customer as it depends on customer's specific distribution*	***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*

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 *Range* *0 – Low Risk* *> 0 – 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 Email Phone – 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 email address and Phone number 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*	***Behavior:*** *Submits their real email address and phone number, and uses their own device without any manipulation.* ***Mastercard data:*** likely has a	***Behavior:*** *Typically m*anipulates device attributes or uses a virtual machine to mask their device. U*tilizes disposable or temporary emails and change email addresses and phone numbers frequently.*

the risk.	large value since we have seen this combination a long time ago.	***Mastercard data:*** resulting in a new Device-email and phone combo, where recently seen combinations have much higher association with fraud.

Device Email 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, 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

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:*** *Typically m*anipulates device attributes or uses a virtual machine to masks their device and IP address. U*tilizes disposable or temporary emails.* ***Mastercard data:*** resulting in a new Device-email and IP combo, where recently seen combinations have much higher association with fraud.

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.