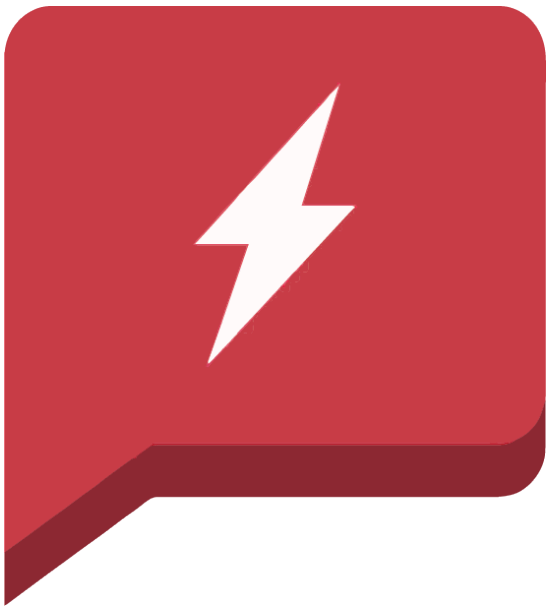
Disclaimer:
The information detailed below and the hypotheses describing that information are not intended to be taken as absolute fact. We are making educated guesses based on research. We will attempt to remain objective at all times.

Adyen is a malleable product. Its security system consists of a set of rules that storefronts can select a subset of and tailor them to their specific needs. We do not know which site uses which rules.

There is an “ultimate Adyen safety guide” at the bottom of this document.



What is Adyen and what are the current circumstances?
Adyen is an EU-based payment processor recently implemented by Foot Locker, Kids Foot Locker, Champs, and Foot Action. We have seen the percentage of orders canceled increase drastically since its release. Adyen is the AIO anti-bot. Its documentation refers to a potential purchaser as a “Shopper” and we will use this terminology throughout this document.

Adyen studies its shoppers information, which it calls “ShopperDNA,” and looks for any minor inconsistencies that may reveal the use of automated software.

You can think of the information involved in ShopperDNA as a profile.

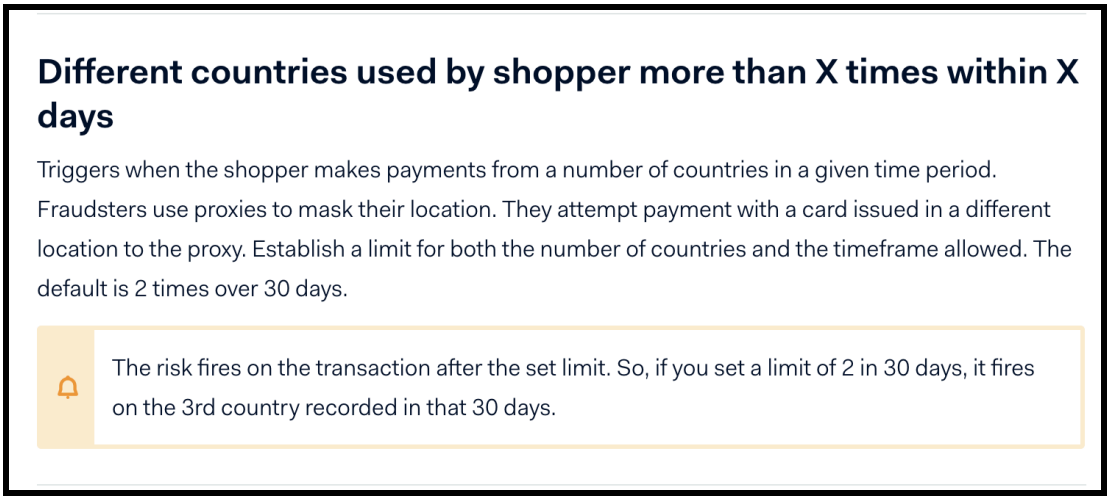
The public components of ShopperDNA include:

- Card Number
- Delivery Address
- Card Holder Name
- IP Address
- Shopper Email
- Shopper Name
- Shopper Reference (“The shopper reference is a unique identifier for a shopper that a merchant provides in the payment request.”)
- Shopper Telephone Number

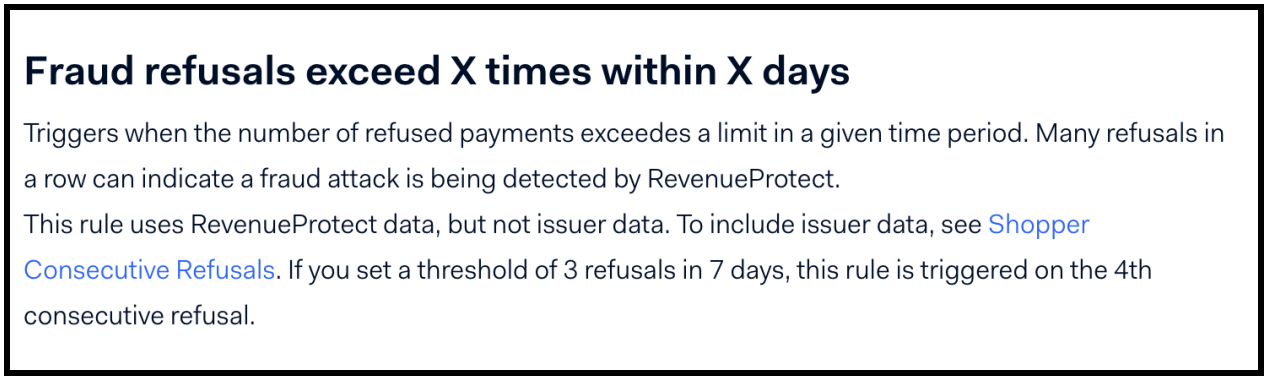
Inconsistencies in any of the above information can result in an immediate cancelation trigger.

The following screenshots are directly from the Adyen ShopperDNA documentation and represent what we believe to be common violations of their ruleset. We will attempt to provide a brief explanation and an overview of potential repercussions.

We do not know which sites are utilizing which rules.



Until the implementation of Adyen a common practice amongst residential proxy providers would be to diversify their geolocation pools for Footsites. One could checkout in the US with a Canada IP. This is potentially no longer the case. If your profile has used a US IP, then if this rule is enabled then it must continue to use a US IP.



This appears to mean that repetitive payment declines / fraud triggers can yield a permanent ban of the Shopper utilizing the given data of their ShopperDNA. *Ensure the card numbers in your profile are 100% accurate.*

High amount velocity

Triggers if a shopper makes more than the specified number of high-value transactions in a given time period.

The storefront can set a threshold of one for their “high-value transaction” at just below the pricepoint of the product it knows Shoppers will be attempting to procure using automated software. Seemingly eliminates the potential for multiples on one profile.

Multiple distinct IP addresses used by shopper more than X times within X minutes/hours/days

Triggers when a shopper uses a number of distinct IP addresses in a given time period. Fraudsters use proxies that switch between IP addresses to hide their identity. This rule identifies these profiles. The default is 2 times over 3 days.

Adyen dynamically determines if an IP address is a shared IP address and does not include these in the rule calculation. This is to reduce the effect that using networks , such as Wi-Fi hotspots have on good users' scores. The shared IP address rule allows you to flag the use of these shared IP addresses if needed.

If this rule is enabled and if your ShopperDNA is linked to multiple IPs (separate tasks even days apart) then you will be canceled. For this reason it appears plausible that *one should assign an IP to a specific profile and use it only for that profile and for that specific site. If your bot permits “Assign specific proxy to task,” then this feature seems more viable than ever.*

This rule also offers an explanation for why people received mass shipping on Toros, but mass cancelations on Grapes utilizing the same information. If your automated software selected a different proxy (likely for Datacenter or ISP services and nearly guaranteed for residential services) and the storefront’s threshold for identification overlap was set to a week, then you were auto-canceled.

Multiple distinct delivery addresses used by shopper more than X times within X minutes/hours/days

Triggers when a shopper uses a number of different delivery addresses in a given time period. Fraudsters often use multiple delivery addresses to commit fraud.

Multiple distinct email addresses used by shopper more than X times within X minutes/hours/days

Triggers when a shopper uses a number of different email addresses in a given time period. Fraudsters often cycle through lists of email addresses to appear legitimate. This rule identifies these profiles. The default is 3 times over 3 days.

Multiple distinct shopper references used by shopper more than X times within X minutes/hours/days

Triggers when the shopper uses a number of different shopper references in a given time period. The default is 2 times over 30 days. The shopper reference is a unique identifier for a shopper that a merchant provides in the payment request. This is usually the User ID. Fraudsters use multiple accounts to appear like separate, and legitimate users. This rule identifies these profiles.

> ⚠ For this risk rule to work properly, it is imperative that merchant's ensure that there is parity between their internal reference numbers/ID associated with a unique user and what they are passing to Adyen via the `shopperReference` field.

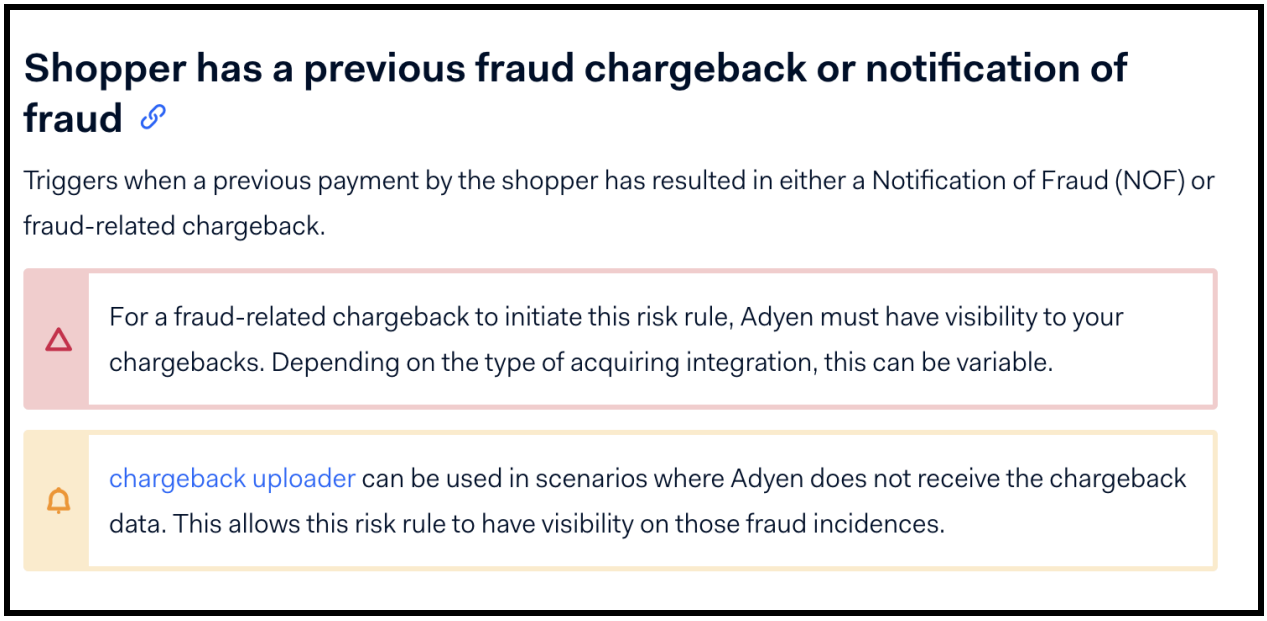
Shopper authorized velocity exceeds X times within X minutes/hours/days

Triggers when a shopper makes a number of authorisations in a given time period. The default is 3 times over 7 days.

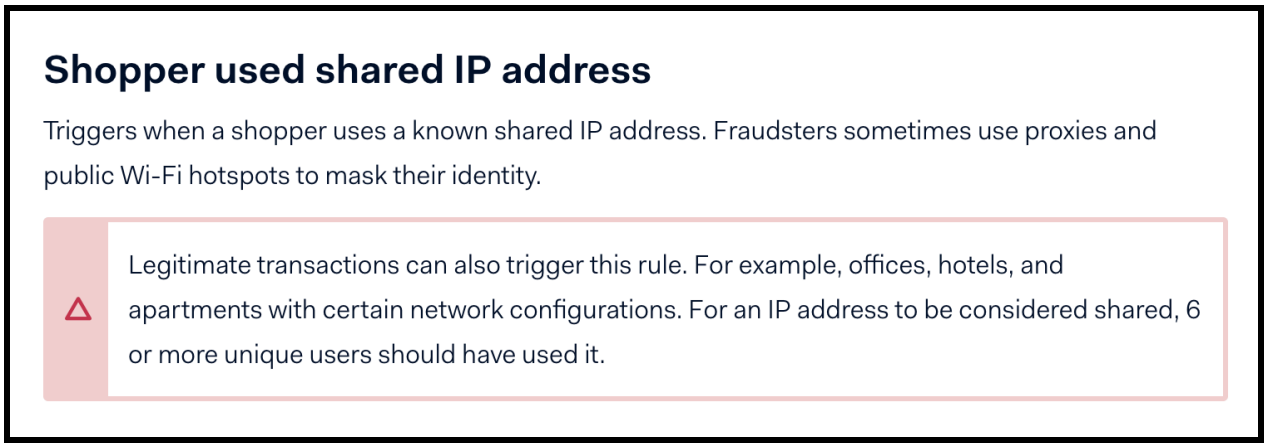
Fraudster attempt many payments in a short time period. While refusal velocity is a stronger signal of fraud, it can be useful to track users who are successfully authorising a high volume of payments. This can indicate a fraud attack that is being undetected by the Issuing banks.

> ⚠ The number of expected authorisations varies based on your business model and vertical. For example, airlines can expect significantly less velocity than businesses based on micro-transactions.

The above rules seem to us to be relatively straightforward (the “reference” again is seemingly a token assigned by the storefront to the session) and if enabled point toward the inability to procure multiple pairs on a single profile, to have information carry over from Shopper to Shopper, and to limit the viability of even slightly altered profile information.



If your profile has been flagged before, then that profile is likely incapable of checking out until the storefront refreshes the information they have cached. On the backend — we were able to find rulesets that the *default value for cached information can be as high as thirty days.*



Determines if the IP linked to your session has been linked to previous sessions operating with different ShopperDNA. ***Renew your Datacenter and ISP proxies for as long as your proxy provider permits.***

Velocity rules

Velocity checks trigger based on the number of transactions a shopper has attempted in a given time. The average number of transactions from a good shopper varies depending on your business, so configure these checks to the behavior of your shoppers.

Adyen also studies the "velocity" at which its Shopper attempts checkout(s). Defined by Adyen as "the number of transactions a shopper has attempted in a given time."

It is important to note that the "given time" described above is determined uniquely by each Adyen client, i.e., each site may be different.

Adyen's velocity rules work at both micro- and macro-levels.

Micro: Adyen looks for the speed at which the information described in ShopperDNA is input into the payment gateway.

Macro: Adyen looks backward at the Shopper's site usage. We are certain it is capable of looking back at least three days at the IP address the Shopper uses as its navigation source.

Card/bank account holder name used more than x times within a time period

Triggers when the number of transactions associated with the same cardholder name exceeds a given number of transactions in a given time period.

Fraudsters often use the same cardholder name when testing cards, so as to more easily automated their process. This check is aimed at detecting when the same name is being used across a set number of transactions.

Card/Bank account number used more than x times within a time period

Triggers when the number of transactions associated with the same card or bank account number exceeds a given number of transactions in a given time period.

Card/Bank account number already used by another shopper

Triggers when the payment method for the transaction has already been used with a different Shopper Reference.

Fraudsters create multiple accounts, and attempt to use the same compromised account with different techniques and attack vectors. This check is aimed at identifying when a payment method is being used across multiple accounts.

Enable this setting across all your merchant-level accounts to provide the most reliable results.

These rulesets, if enabled, create a seemingly paradoxical relationship between number of tasks and number of pairs shipped. Unique, correct information is of the utmost importance. Checkouts that occur with unique information that ***is not repeated in any other session*** have the highest likelihood of bypassing the storefront's ruleset. Again, if enabled, signs point toward one profile (with a real card) per IP per site.

Shopper email used more than x times within a time period

Triggers when the number of transactions associated with an email address exceeds a given number of transactions in a given time period.

Fraudsters use the same email for clusters of transactions because creating new emails is time intensive. This check allows you to set velocity limits on any email address.

Shopper delivery address used more than x times within a time period

Triggers when the number of transactions associated with a shopper delivery address exceeds a given number of transactions in a given time period.

Fraudsters often use the same shipping address to receive stolen goods. You can set velocity limits on any shipping address to prevent fraudsters from using it.

Shopper IP used more than x times within a time period

Triggers when the number of transactions associated with an IP address exceeds a given number of transactions in a given time period.

Fraudsters often use the same IP address for consecutive fraudulent transactions. This could be while they are attempting different card details, or techniques. This check allows you to set velocity limits on any particular IP address.

These rulesets provide an explanation as to why many users are reporting having one pair ship. We do not know if Foot Locker, Kids Foot Locker, Champs, and Foot Action amalgamate the information they receive, though in our opinion it is likely they do.

Shopper initiated a transaction more than X times within a time period

Triggers when the number of transactions initiated by a shopper exceeds a given number of transactions in a given time period. The default setting 5 times over 90 minutes. Unlike other velocity checks, which are based on a single matching attribute, you can base this check on:

1. Device Fingerprint: A technique used to identify shoppers by making a fingerprint of their device/browser. In most cases, the fingerprint is unique for each device or browser. Contact Support Team to ask about using device fingerprinting with your account.
2. Persistent Cookie: A unique identifier stored in different places on the shopper's device and across browsers. To turn on persistent cookie tracking for your account contact Support Team.
3. Shopper IP
4. Shopper Email Address

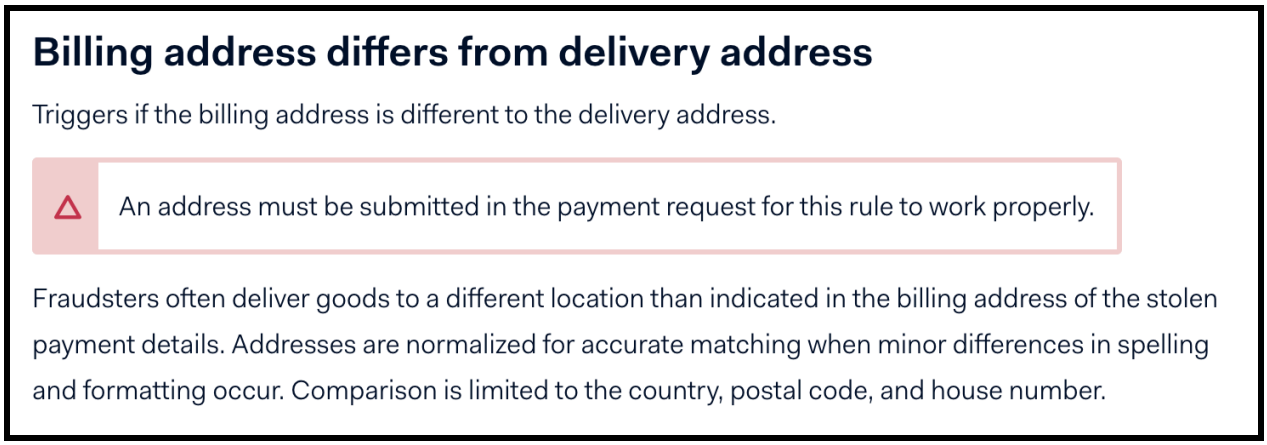
If enabled then one must consider drastically raising delays. If your delays are 3000/3000, then you're attempting 5 transactions in 15 seconds.

The default setting of 5 times over 90 minutes is most likely changed by footsites. They would acknowledge that people have a tendency to refresh pages, smash submit, etc., given the server workload caused by the influx of automated traffic.

Consistency rules

Analyze shopper data for fraud by comparing transaction data points with each other.

Consistency rules combine the information gathered by the ShopperDNA and the Velocity rules and synthesize the data.



Self explanatory if enabled.

Email address and shopper name comparison

Triggers if the provided email address does *not* match (or partially match) the `cardholder name` (if provided) or the `shopper name`.

Email is likely to be fake or automatically generated

Triggers if the provided email address is likely fake or automatically generated. Fraudsters set up scripts to automate the creation of email addresses. Our prediction algorithm analyzes email address across our entire network and correlates certain attributes with fraud and known card-testing schemes.

Using this data, our risk system determines the probability that the email address is to be fake. You can set a separate risk score for payments that are **Somewhat likely to be fraud** and **Very likely to be fraud**. These scores will increase the total risk score of the payment.

If John Doe checks out and his email does not resemble something along the lines of JohnDoe@gmail.com, then this rule would trigger. It may be beneficial to make real emails that resemble the names utilized in your ShopperDNA, e.g., JohnDoe@gmail.com for John Doe profile, JohnnyDoe@gmail.com for Johnny Doe profile.

Fraudulent behaviour on payment page

Triggers if the algorithm has detected behavior in the card number and/or CVC fields that appear to be scripted.

Fraudsters use scripts to test a set of cards. This risk rule analyses time taken, key-based, and mouse-based behaviors of users interacting with the payment fields.

Using this data, our risk system determines the probability that the behavior is fraudulent. You can set a separate risk score for payments that are **Somewhat likely to be fraud** and **Very likely to be fraud**. These scores will increase the total risk score of the payment.

This risk rule is available for if you are using Client-Side Encryption (Merchant-hosted and Adyen-hosted, version V0.1.12 or higher). It is not available for Client-Side Encryption (JavaScript) and direct API integration types.

Transaction time

Triggers if the transaction falls within one of the configured time frames.

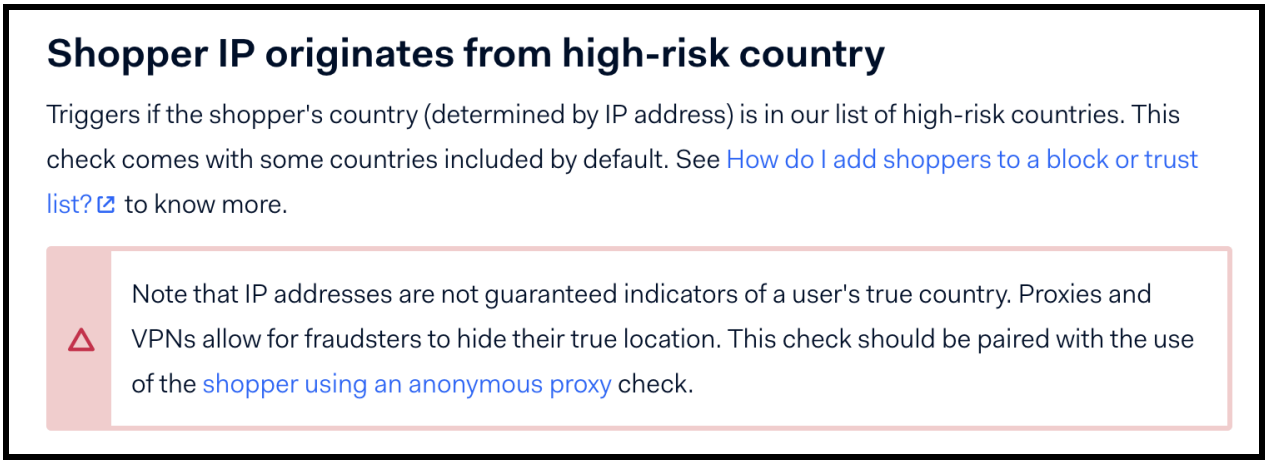
Fraud can spike at specific times when legitimate transactions are limited, like during the night. This rule allows you to increase or decrease the risk score accordingly.

Adyen analyzes and determines the human nature of the checkout process. It synthesizes the checkout duration, the movements of the Shopper's mouse, whether or not the input ShopperDNA was auto-filled and/or copy and pasted. This rule being enabled would explain why some users have reported cancelations on manual orders.

Payment method

Triggers based on the payment method used. Some payment methods have more instances of fraud. This check lets you change the risk score based on the payment method behavior.

Likely pertains to VCCs. All signs point to hard cards being the way.



Harkens back to ShopperDNA, where we explained IP Geolocation. If enabled, then any IP with a geolocation which the storefront determines high-risk would be flagged. Our guess is that this has to do with shipping location.

Disclaimer:
The following guide contains many assumptions. Namely, that the ShopperDNA rulesets listed above are enabled, that you check the product out, and that you have bypassed the "fraudulent behavior on payment page" rulesets found on page 13.

The following guide pertains to a Shopper who wishes to be as safe as they can be. We understand the guidelines below greatly inhibit your ability for a large cook. They are neither recommendations nor requirements, simply potential guidelines determined by our observations.

We make no promises of its efficacy.

We are sure we have missed plenty.

The Ultimate Adyen Bot Safety Guide

1. One task per profile.
2. Do not use the same profile on multiple sites.
3. Use a real email that appears similar to the name in your profile. No catchalls.
4. Assign a specific proxy to a profile and use the IP nowhere else.
5. Do not run any test tasks with an IP that you intend to use to attempt to checkout.
6. Increase delays drastically.

With love,
@botglen
@judgements