Anti-Fraud Functionality

Most of our anti-fraud checks are performed before the transaction is sent to an acquirer bank for authorisation process, after all the transaction details (including any additional authentication such as 3D Secure) have been gathered at Telr's end.

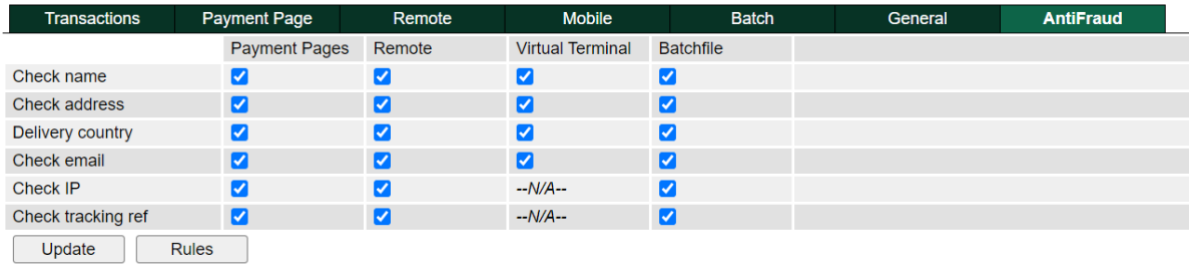
Antifraud rules can be created or managed through Merchant admin and Sysadmin both through different options available, like Country control, Processing rule, card limit etc.

Apart from frontend options, antifraud rule and functions can be created and managed from the backend code as well.

In addition to the standard anti-fraud code that is used across all merchants and acquirers, there is an option for custom code to be added for specific merchants/acquirers.

1. Blacklist scanning:

- System scans the blacklist for matching entries, unless any custom anti-fraud module indicates that the blacklist can be skipped.
- By default, "Blacklist" checks in the setting is enabled for all the stores, which is under 'AntiFraud' option in Sysadmin merchant detail page (Please check below screen shot)



- If any of the check is removed from the Antifraud options, that information type will be skipped in the scanning during the transaction and customer can use any blacklisted details in the payment.

2. BIN block check:

- System checks for blocked BINs (Card number prefixes - merchant config can set that specific card ranges are not to be accepted)
- Below are DB update made for stores in store integration table. Bin block list are shared by compliance team to IT team to set at DB.

	store_id	integration_type	name	value	time_stamp
1	13913	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
2	13916	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
3	13929	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
4	13962	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
5	13964	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
6	14052	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
7	14069	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
8	14117	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
9	14136	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647
10	14163	0	conf_binblock3	517003,547395	2020-11-02 16:51:54.647

3. Proxy IP check:

- System checks if any proxy IP address is used for the customer from the payment pages (checking for possible use of proxies to try and conceal location)
- We are maintaining a mapping of “Country IP” and “Country Code”. It checks against the Billing IP country of the customer. If the IP is not matching transaction will be blocked.
- If we are Removing this check from the backend, customer can make transaction through any country by providing different billing country detail on the payment page. We will be unable to keep a hold on any transaction through its location.

4. Country control check:

- System will check the customer IP country and Billing IP details and process the transaction as per the rule set in the “Country control” option at store level.
- If the action on the country is set as “On Hold” and customer is trying to make a payment through that country, our system will identify the rule set in Country control and hold that transaction.
- At present the severity of country control is handle in way that, the highest severity is considered among Merchant admin and sysadmin.
- Example:
  a. On sysadmin, “Bosnia” is On-Hold and under Merchant admin it is set as “No Action”, preference will be given to On-Hold as it has higher severity then ‘No Action’.

b. On sysadmin, “Bosnia” is On-Hold and under Merchant admin it is set as “Block”, preference will be given to Block as it has higher severity then ‘On-Hold’. As this ‘Block’ is set by the merchant from merchant admin, it will only affect that store.
c. On sysadmin, “Bosnia” is Block and under Merchant admin it is set as “On-Hold”, preference will be given to Block as it has higher severity then ‘On-Hold’.

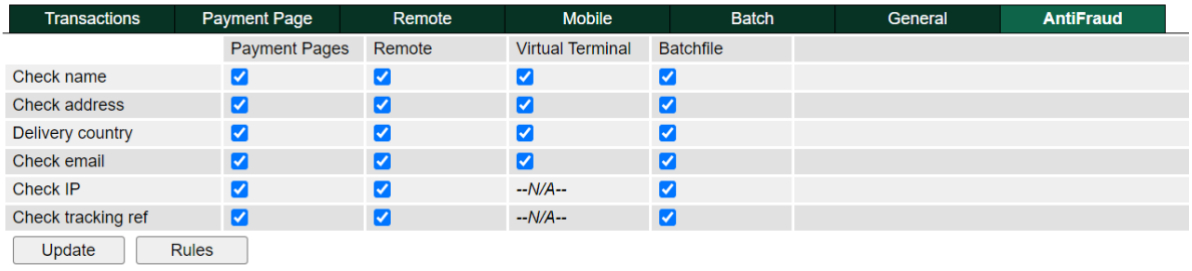
5. **Sanctioned Countries:**

System will check the customer IP country and Billing IP details and process the transaction as per the rule set in the “Sanctioned Countries” option at System Level.

Only one user has access to this option.

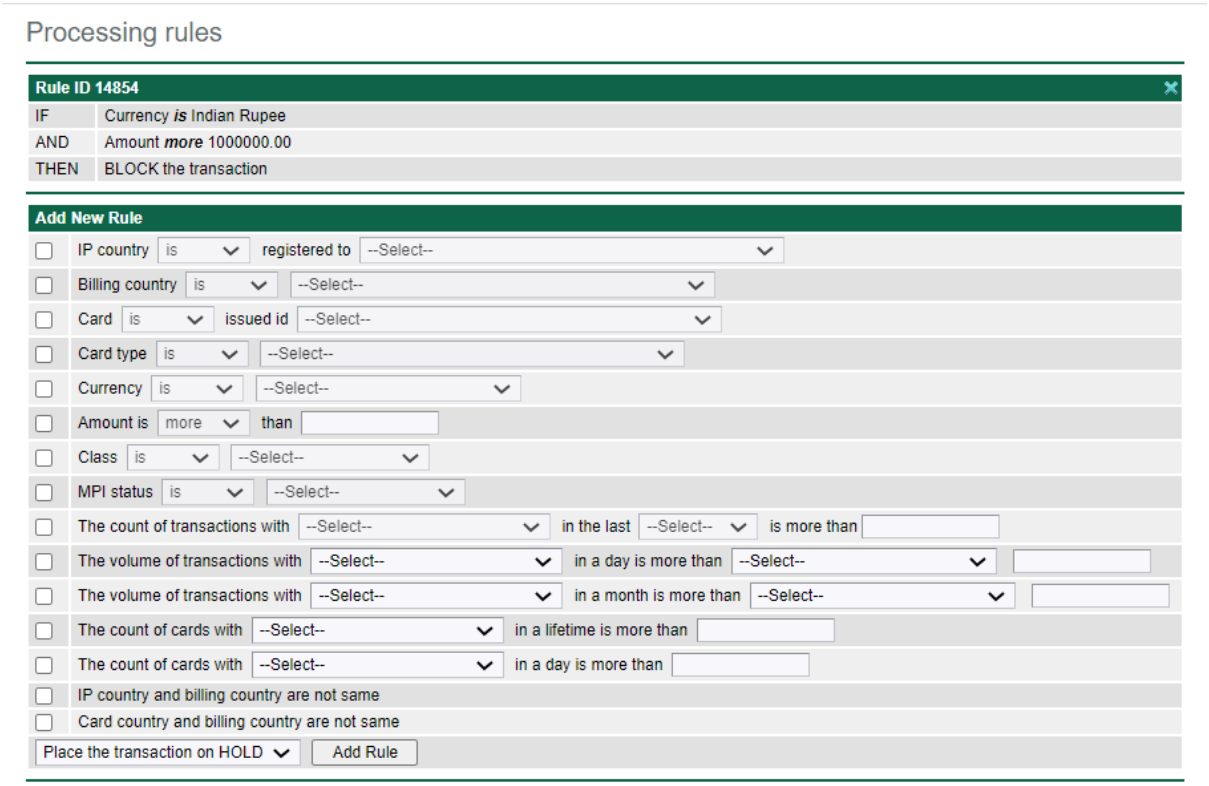
6. **System email address check:**

- For every transaction our system reviews the email address
- If email address does not appear valid, then flag transaction to be placed on hold.
- If email address is blacklisted or used in previous suspicious transaction, that transaction will be blocked.
- If email check is removed on any store from Sysadmin, our system will stop scanning the email address for every transaction on that store and customer can use any “Blacklisted email ID” while making the payment.



7. **Anti-Fraud Rule Check:**

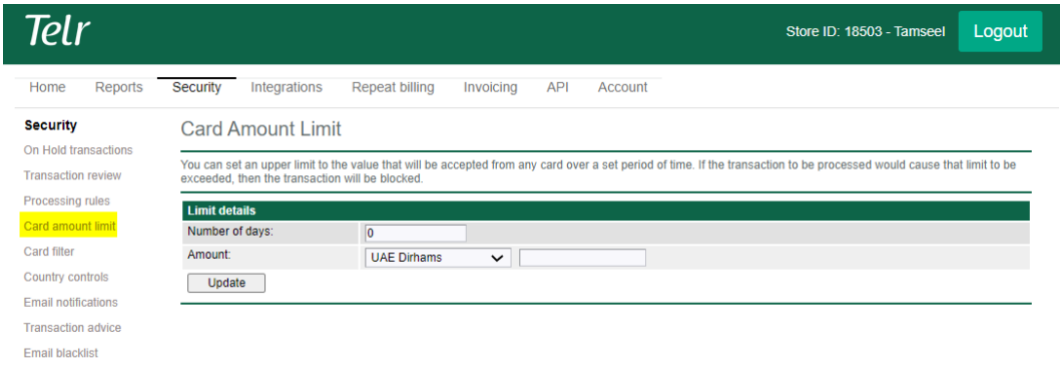
- AntiFraud Processing rule can be created from Sysadmin or by merchant through Merchant admin “Processing rule” option.
- Multiple rules can be created through Processing rules option, you can see rules option in the below screen shot.



- System checks any specific anti-fraud rules (system wide and store level), and update the transaction status as per the rules (On Hold or Block)
- Rules created by Sysadmin on any store cannot be accessed or changes by merchant through merchant admin.
- This option gives us and merchant to reduce the fraudulent transaction attempt by adding additional antifraud rules as per the Card type, Card Country, Transaction Volume, Number of attempts, MPI Status etc.
- Telr team sets a Processing rule on a store or Across stores as per the Global rule or depending on the merchant's business.

8. Card Amount Limit:

- Merchant can set transaction limit on any card through "Card Amount limit" option in 'Merchant admin'. This can be enabled only through merchant admin by merchant.
- For every transaction system checks if the merchant has configured any transaction limits to be checked per card (such as maximum spend from the same card within a set period)
- As per the set limit transaction reviewed and will be allowed or blocked.



9. DNS Blacklist Check:

- There is a DNC check implemented in the backend coding, to check the IP address merchant system IP.
- System checks known DNS blacklist providers (such as Spamhaus and SORBS) to see if the IP address is associated with any known open proxy servers or otherwise compromised systems.
- If the IP is identified from proxy servers or otherwise compromised systems, it will block the request to enter in Telr System.
- Removing this check will open our system to open servers and compromised system, increase the chances of any kind of system attack.

10. Aggregator Rules Check:

- System checks aggregator rules for every transaction by default, this check is implemented from the backend coding. Non GCC card, electronic business, Transaction amount more 5000 AED and transaction is not 3ds then it will on hold.
- Any changes in this check will affect the transaction check for GCC card, business type control and amount control.

11. Custom Anti-Fraud check:

- For every transaction system checks any custom anti-fraud modules defined for the merchant. Any Antifraud changes through custom ‘C’ code created or Hardcoded from the backend, this does not include the rule created form front end.
- This rule or Antifraud check can be removed or managed only from the backend code.

12. Refund Checks:

- Check if the merchant is blocked from doing refunds (set if requested by compliance), block any refund request if they are.

- Currently there is no UI element for setting this. This can be implemented only from the back end.

13. <u>Country control:</u>

- For each transaction, all rules that relate to any country code associated with the transaction (such as card issue country, customer billing country, IP address country) are checked.
- The rules can trigger any of the following actions:

  - Hold transaction unless all countries are from the same region.
  - Hold transaction, unless all countries matches.
  - Hold transaction.
  - Block transaction, unless all countries are from the same region
  - Block transaction, unless all countries match
  - Block transaction

- The most restrictive result of any check is the one that is taken as the result. So, for example, if there is a system rule for a country that says block, but the merchant adds a rule for the same country that says hold, then the result would always be block.
- System checks against some fixed generic rules, such as card country not matching IP country. If the card country IP and Customer's IP, then system will block the transaction.
- If IP check is removed, we will not have control over card IP and location of the customer. Transaction can be made through any blocked location and card.

14. <u>SBL:</u>

- The short-term blocking list contains entries that can either block a transaction or flag the transaction to be placed on hold if it is authorised (if both a hold and a block match are found, then the block result will take precedence).
- The main difference between this and the standard blacklist, is that entries on the SBL automatically expire over time. Entries on the blacklist are permanent unless manually removed from the backend.
- The SBL also tracks more components of the transaction, not just the card number and email, but also customer name and address.
- To help track similar addresses and spelling variations etc, the names and addresses are converted to metaphone representations of the text before being checked. In addition, after conversion to metaphone, any duplicated words are removed, and the final word list is sorted into alphabetical order.
- SBL restrict the customer to use fraudulent details continuously at the same time, the details get blacklisted for short period and if the same details are used the transaction will be block.

- Removing the SBL blocking will allow the user to make multiple attempts with the same details which got decline by banks or Telr for suspicious reason and will increase the chance of fraud transaction.

SBL Checking list:

- When checking the SBL for matches, the system will scan back for any matching entry that was added to the list within the last 30 minutes. Anything added more than 30 minutes prior to the transaction will not affect it.

SBL Adding entries to the list:

- Once the authorisation process is completed, the result of the transaction is checked.
- If the result was a block (because of matching any anti-fraud rules, including SBL checks, or a block response from an acquirer such as lost/stolen card) then a new SBL entry is added with the transaction details, and a status indicating any match should result in the matching transaction also being blocked.
- If the result indicated the transaction should be put on hold, then a new SBL entry is added with the transaction details, and a status indicating any match should result in the matching transaction also being placed on hold.
- This process of feeding results back into the SBL allows for tracking of people that may be trying (for example) to process using different cards or emails etc to try and get a fraudulent transaction through the system. The more they keep on trying, the more information is added into the list helping to block their attempts.
- Checks the SBL (Greylist) for any matching entries. If yes, transaction will be declined.
- Our system matches the transaction details with any previous suspicious entries and decline or put on hold the transaction depending on the scenarios.

15. <u>Blacklist:</u>

- There are two blacklist tables, one for dealing with card numbers (via the card vault) and one for text-based details such as email address.
- At the start of a transaction each of the following details are checked to see if a matching entry exists on any of the blacklists:

  - Card Number (via the card vault)
  - Card BIN (First 6 digits)
  - Email address
  - Email domain
  - IP address

- If a match is found to any of these, then the transaction will be blocked.

- This will be the system wide permanent blacklist and can only be removed by IT team from the backend after managements approval.

16. <u>Transaction Review:</u>

- Our system puts transaction under review of the merchant, if system identifies the transaction as suspicious.
- For example: If a customer tried to make a payment and it got decline due to 3D secure authentication and the customer tried again using the same payment details and the transaction go through successfully, then the system will put the transaction under review option in Merchant admin and notify the merchant to review it. If merchant feels the transaction is suspicious , they can cancel the transaction or let it be without any action and it will be processed further for settlement as a normal transaction.
- Review is not same as On-Hold transaction. Under review system will only inform the merchant to verify the transaction and if no action is taken then it will be processed further.

17. <u>AutoBlock:</u>

- Any entry on the blacklist can have a flag of 'autoblock' set. If a match is made to any existing entry that has autoblock, then the current transactions card number and email address are automatically added onto the blacklist (if they don't already exist). These new entries will themselves have the 'autoblock' flag set.
- For example, if a transaction with email 'test@test'.com' and card '4111 1111 1111 1111' matched an existing card number entry with autoblock set, then the email address will then be added to the list. If the same email address, then tries again but with a different card number, as that email is now flagged as 'autoblock' then the new card number will also be added. This is similar to the way the SBL works, but only deals with card number and email, and entries do not automatically expire after time.
- Most of the automated ways of ending up on the blacklist (such as a response from an acquirer that the card attempts were reported as lost) do not result in blacklist entries with 'autoblock', they will just be standard blacklist entries. It is generally when adding data from known confirmed fraud or data exposed from known breaches that the values will be added with 'autoblock' set.

- Below are the reasons that trigger autoblock,

  - Card has been reported as lost.
  - Card has been reported as stolen.

- Blocked by issuer due to suspected fraud.
- Autoblock triggered due to card/email used matching with entry which has autoblock set on it.
- Compliance Manually Setting the Autoblock on Card and Email.
- Used a card on the prohibited IIN list.

18. <u>Test transactions:</u>

- Transactions in test mode, or using any of the known test card numbers, will not be added to the blacklist.