Elavon Payment Gateway-Fraud Management

User Guide

Version: 1.1

Table of Contents

1 About This Guide

This section outlines the purpose and aim of the guide, target audience, any source materials or terminology used, and a general document description. Please note that this document is regarded as confidential and is for customer use only. It has been supplied under the conditions of your payment-processing contract.

1.1 Purpose

The purpose of this guide is to provide all of the details required to work with Fraud Management.

1.2 Audience

The target audience for this guide is users of Fraud Management.

1.3 Prerequisites

In order to use this guide, you should have experience with and knowledge of the following concepts:

- Knowledge of the Reporting Tool

1.4 Related Documents

In addition to this guide, you can also refer to the following documents in the Elavon Payment Gateway documentation set for information about the Elavon Integration service:

- Reporting User Guide

1.5 Conventions

Elavon Payment Gateway documentation uses the following conventions:

Note: Tips or advice for the user.
Caution: Important note. Potential financial impact.

Conventions	Description	Example
Blue Italic or Plain Type.	Hyperlinks and cross-references.	For more information see Table 1.
Italics.	Names of other guides.	*Elavon Auth Developer's Guide.*
Courier New.	Program code, screen messages, directory files, and file names.	<comments></comments>
Courier New.	Placeholder for element names, field values or user input.	*card_holder_name*
BOLD CAPS.	Error and warning messages.	**101 / REFERRAL B.**

2 Introduction

What is Fraud Management?

Fraud Management is designed to assist merchants with managing fraud at the point of sale by identifying negative data, identifying potential conflicts within a transaction's data and checking each transaction for patterns in real time. Fraud Management is configured through Reporting by the merchant. It uses criteria entered in the Fraud Management section of Reporting to assess transaction data. The criteria take the form of rules which are applied to calculate a score for the transaction. The result of the individual Fraud Management rules can be returned in real time along with an overall score for the transaction.

Note: Fraud management rules are applied on a sub-account basis. For more information on sub-accounts, please see the *Elavon Auth Developer's Guide*.

There are 2 types of Fraud Management:

- TSS (Transaction Suitability Scoring).
- TSS with Autocheck.

2.1 TSS (Transaction Suitability Scoring)

TSS calculates the Fraud Score based on the rules that the merchant has set up in Reporting. The score is then returned in the transaction response and can be seen in Reporting in the Transaction Details.

TSS is an advisory service; Elavon Payment Gateway will not decline a transaction based on the score returned. However, the merchant can handle the transaction as they wish based on the score returned.

There are two ways in which the merchant can do this:

- A special Fraud Management transaction called a TSS transaction can be sent to Elavon Payment Gateway to verify the fraud score before the authorisation request is sent. In this way, the merchant receives the transaction score before the authorisation has been fulfilled and can decide based on this, whether to proceed with the transaction. The TSS transaction

request is detailed in the *Elavon Auth XML Definitions Guide.*

- If the merchant does not use the TSS transaction, the results of the check will still be returned as part of the authorisation response. At this point, if the merchant deems the score to be unacceptably low, they can choose to void the transaction (or decide not to proceed to settlement if they are using delayed settlement. For more on delayed settlement please see the *Elavon Auth Developer's Guide*).

Note: Unless the account is configured for TSS with Auto Check (as described below), transactions processed through the Reporting Terminal will use the latter option; the score will be stored in Reporting along with the transaction results and can be checked by the merchant after authorisation.

2.2 TSS with Auto Check

Unlike TSS, TSS with Autocheck allows the merchant to configure their account to allow transactions to be declined based on the fraud score returned. A merchant using TSS with Autocheck will configure their Fraud Management rules as usual. However, they will also have an extra configuration setting called "Autocheck Enable/Disable" which will allow them to specify that the transaction should be declined if the check fails (or in the case of some rules, if the result is below a certain score). A transaction that meets the rejection criteria will decline and a 107 result will be returned. The transaction will not be sent for authorisation. The Configuration of these rejection rules is further discussed in "Setting up the TSS with Autocheck Option".

3 Fraud Management Zones and Rules

This chapter describes the following:

- Fraud Management Zones.
- Fraud Management Rules.

3.1 Fraud Management Zones

There are four Fraud Management zones:

- **Zone 1000 - Transaction Screening.**

The rules in Zone 1000 compare data in the transaction against data supplied by the merchant in the Fraud Management section of Reporting. For example, a merchant may list a particular billing country so that all transactions with that billing country will receive a particular result. These checks are merchant specific in that the data that is listed will be unique to every merchant and the merchant also specifies the result to be returned should a particular value be sent in the transaction.

- **Zone 2000 - Data Sanity Checking.**

The rules in Zone 2000 compare certain fields in the transaction against other fields in the transaction. For example, one of the Zone 2000 rules checks if the shipping country and billing country differ. These checks are common to all merchants in that they do not require any specific input from the merchant ; the merchant simply needs to switch the rules on.

- **Zone 3000 - Data Pattern Checking.**

The rules in Zone 3000 compare data in a transaction against data from previous transactions. Some of these checks may require additional input from the merchant in the form of parameter configuration.

- **Zone 5000 – Post Auth Checking.**

The checks in Zone 5000 are based on checks that occur during the authorisation process. The results of these checks are based on the various responses from the bank and will not be known until after authorisation.

Note: It is important to remember:

- All the checks are completed in real time and each individual rule generates a score in the range 0 to 9. Fraud Management works on the basis that the higher the score the lower the risk.
- An overall score is calculated from the scores generated by the individual rules.
- Each rule has a weight that determines the importance of the rule in the overall score (the formula for the calculation of the overall score is provided in section 5.1 Calculating the Overall Fraud Score).

3.2 Fraud Management Rules

3.2.1 Zone 1000

The checks in Zone 1000 compare data in the transaction against data supplied by the merchant in the "Fraud Data" section. For example, if a merchant has experienced a lot of fraud from a particular billing country, they can list this billing country and specify a low score to be returned for the "High Risk Billing Country" rule should the billing country match this value.

Code	Title	Format	Length	Description
1000	High Risk Card number.	0-9	12-19	This can be used to flag card numbers that have been associated with fraud in the past. The card number sent in the TSS and /or auth request will be compared to the list of values stored here.
1001	High Risk Cardholder Name.	a-z A-Z ""_-‘	0-50	This can be used to track and flag cardholder names that have been associated with fraud in the past. The cardholder name sent in the TSS and/or Auth request will be compared to the list of values stored here.

Code	Title	Format	Length	Description
1002	High Risk Customer Number.	a-z A-Z 0-9 –“”_.,+@	0-50	Customer Number is an optional field in which the merchant can store data that is meaningful to them, for example a customer reference. This rule allows merchants to track and flag Customer Number values. For website integrations, the value sent in the “custnum” (remote) or “CUST_NUM” (redirect) field in the TSS and/or Auth request will be compared to the list of values here. If you are using the Reporting Terminal, the relevant field is called “Customer Number”.
1003	High risk Variable Reference.	a-z A-Z 0-9 –“”_.,+@	0-50	The Variable Reference is an optional field that can be used for values that are important to the business for example mobile number, car registration, first time buyer. This rule allows merchants to track and flag these values. For website integrations, the value sent in the “varref” (remote) or “VAR_REF” (redirect) field in the TSS and/or Auth request will be compared to the list of values here. If you are using the Reporting Terminal, the relevant field is called “Variable Ref”.
1004	High Risk Shipping Area.	a-z A-Z 0-9 –“”_.,+@	0-30	This rule allows merchants to track and flag shipping address postcodes. For remote website integrations, the value in the “code” tag within the “address” (type “shipping”) tags in the TSS and /or Auth request will be compared to the list of values here. For redirect website integrations, “SHIPPING_CODE” is the relevant field. In the Reporting Terminal, the field is called “Shipping Code”.
1005	High Risk shipping country.	Predefined.	Predefined.	This rule allows merchants to track and flag shipping countries. For remote website integrations, the value in the “country” tag within the “address” (type “shipping”) tags in the TSS and /or Auth request will be compared to the list of values here. For redirect website integrations, “SHIPPING_CO” is the relevant field. In the Reporting Terminal, the field is called “Shipping Country”.

Code	Title	Format	Length	Description
1006	High Risk Billing Area.	a-z A-Z 0-9 “”.,/	0-30	This rule allows the merchant to track and flag billing codes. Please note that the Billing Code field can be used for the billing address postcode but it can also be to send the additional information required for Address Verification Service (AVS) checking. For more information on AVS please see the *Elavon Auth Developer's Guide.* For remote website integrations, the value in the “code” tag within the “address” (type “billing”) tags in the TSS and /or Auth request will be compared to the list of values here. For redirect website integrations, “BILLING_CODE” is the relevant field. In the Reporting Terminal, the field is called “Billing Code”.
1007	High risk Billing Country.	Predefined.	Predefined.	This rule allows the merchant to track and flag billing countries. For remote website integrations, the value in the “country” tag within the “address” (type “billing”) tags in the TSS and /or Auth request will be compared to the list of values here. For redirect website integrations, “BILLING_CO” is the relevant field. In the Reporting Terminal, the field is called “Billing Country”.
1008	High Risk IP Address.	0-9 IP address in X.X.X.X format.	[1-3].{1-3}.{1-3}.{1-3}	This rule allows the merchant to track and flag a table of specific customer IP addresses. This is compared against the value sent in the “custipaddress” field in the TSS and/or Auth Request.
1009	High Risk Product ID.	a-z A-Z 0-9 –“”_.,+@	0-50	Product ID is an optional field in which the merchant can store data that is meaningful to them, for example a product reference number. This rule allows the merchant to track and flag a table of Product IDs. For website integrations, the value sent in the “prodid” (remote) or “PROD_ID” (redirect) field in the TSS and/or Auth request will be compared to the list of values here. If you are using the Reporting Terminal, the relevant field is called “Product ID”.
1010	High Risk issuer country.	Predefined.	Predefined.	This rule allows the merchant to track and flag a table of specific card issuer countries. The card issuer country returned by Elavon Payment Gateway in the transaction response message will be compared to the list of values here.

Code	Title	Format	Length	Description
1011	High Risk BIN Range.	0-9	0-12	The BIN range is the first 6 digits of the card number. This rule allows the merchant to track and flag BIN ranges. This values listed here are compared with the first 6 digits of the card number in the TSS and/or Auth Request.
1012	Check 3DSecure Result.	0,1,2,5,6,7	1	The result generated is based on the ECI value returned for a transaction that has been processed through 3DSecure.
1013	Partial Billing Area.	a-z A-Z 0-9 “”.,/	0-50	Like rule 1006, the “billing code” field in the TSS and/or Auth request will be compared to the list of values here but this rule differs slightly. For rule 1006, the billing code must match the listed value exactly; for this rule, if part of the billing code sent in the transaction matches one in the list, the score assigned to the listed billing code will be returned for this rule.
1100	Shipping and Home Countries.	Predefined.	Predefined.	This rule compares the Shipping Country field in the TSS and/or Auth request with the customer’s home country (as dictated by their IP address). If the values match, the check returns 9, otherwise 0 is returned.
1101	Billing and Home Countries.	Predefined.	Predefined.	This rule compares the billing country field in the TSS and/or Auth request against the customer’s home country (as dictated by their IP address).. If the values match, the check returns 9, otherwise 0 is returned.
1200	Maximum Ticket Size	Predefined.	Predefined.	The maximum ticket size is an upper limit on the ticket size which is configured by currency in the Advanced configuration for this rule (see Setting up the TSS Option). This check compares the maximum ticket size against the amount in the TSS and/or Auth request. If the amount is below the maximum ticket size, the check returns 9, otherwise 0 is returned.
1201	Maximum Ticket Size	Predefined.	Predefined.	High Risk times can be configured in the Advanced configuration for this rule (see Setting up the TSS Option). This check compares the time of the transaction against these high risk times. If the transaction time does not match these times, the check returns 9, otherwise 0 is returned.

As discussed above, each rule that is activated in Fraud Management will return an individual score which is used to calculate the overall score. For any 1000 rule that requires the merchant to list

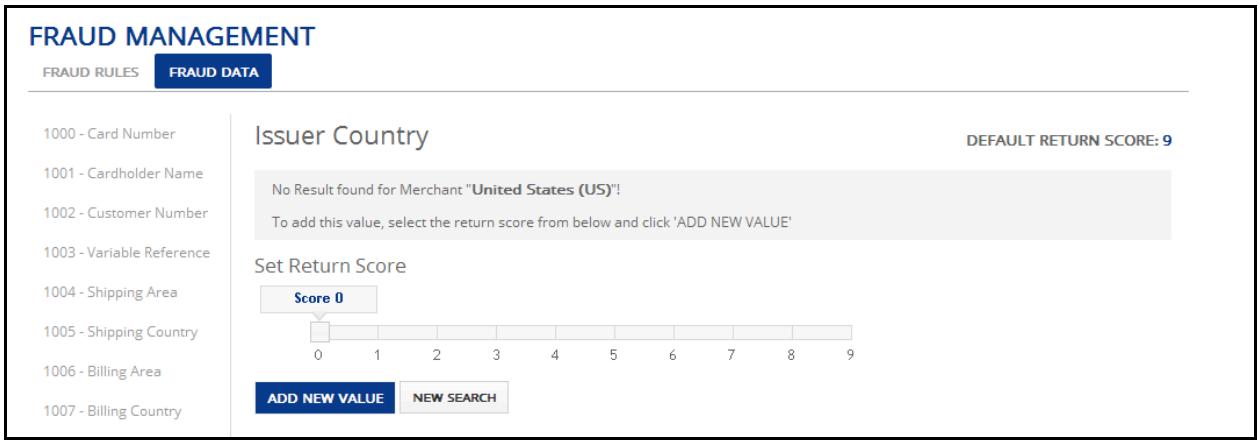
values in the Fraud Data section (i.e. rules 1002 – 1011 and rule 1013), the merchant specifies the score that will be returned for the rule if the transaction field value matches a particular value in the list. The value can be assigned a score between 9 and 0. In keeping with the Zone 2000 and 3000 checks (for which the scores for the various scenarios are predetermined), 9 is generally considered to indicate a high risk while 0 indicates low risk. A scale is provided in the "Fraud Data" section for each value entered. This scale allows the merchant to assign a score. A default score can also be assigned to each rule; this is the score that will be returned if the transaction field value does not match any item in the list.

To access the Fraud Data section:

1. Select **Fraud Management** from the main Reporting menu.
2. Click **Fraud Data.**

To assign a Fraud Score value:

1. On the left of the Fraud Data screen, select the rule for which you want to add a new value.
2. Before a value is added, Fraud Management searches for the value to check if it has been added already for this rule. Enter the value that you wish to add into the text box and click **Go**. If the value does not exist for this rule, a “No Result Found” message should be displayed.



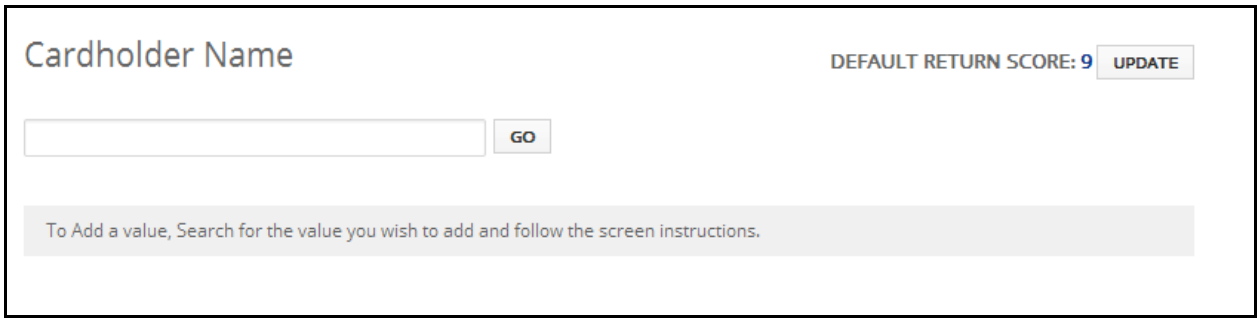
3. Select a TSS score from the scale provided. This is the score that will be returned should the relevant field of the transaction (in this case, Issuer Country) match the value that you have inputted.

4. Click **Add New Value.**

To change the Fraud Score for an existing value:

1. On the left of the Fraud Data screen, select the rule for which you want to modify a value.

2. Enter the value that you wish to search for in the text field provided and click **Go**.

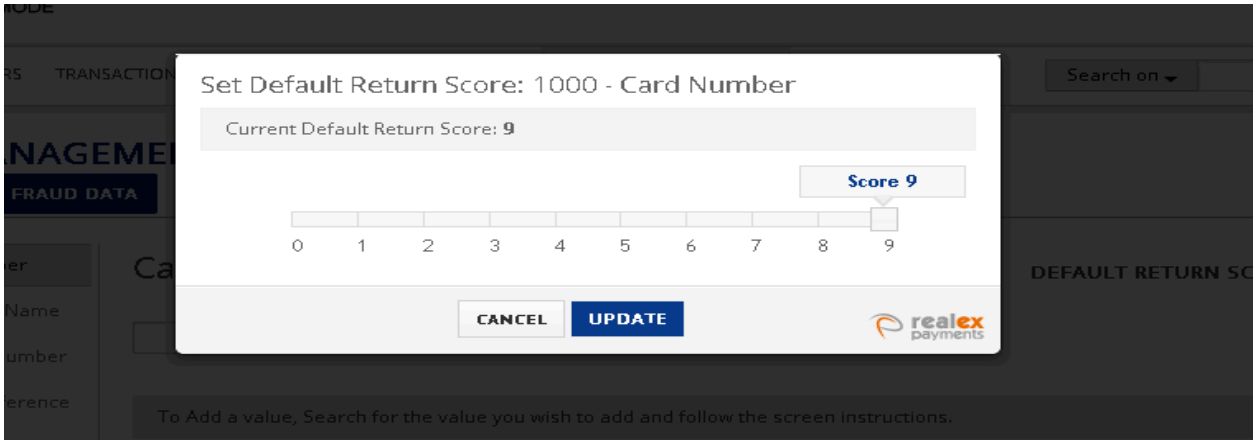


3. If a Fraud Score already exists for this value, you will be presented with a "Result Found" message and a scale that shows the current assigned score. You can amend the score by selecting the required value on the scale and clicking **Update**.

4. If a Fraud Score does not exist for this value, you will be presented with a "No Result Found" message. If required, you can add the value as described above.

To modify a Default Score:

A default score will be returned for a rule if the value in the relevant field does not match any of the values that you have listed. This default Fraud Score can be set for each rule follows.



1. On the left of the Fraud Data screen, select the rule for which you want to set a default score.
2. Click on the **Update** button beside “Default Return Score”.
3. A scale will appear with the pointer set on the current default score for that rule. You can change the default score by selecting the required value on the scale and clicking **Update**.

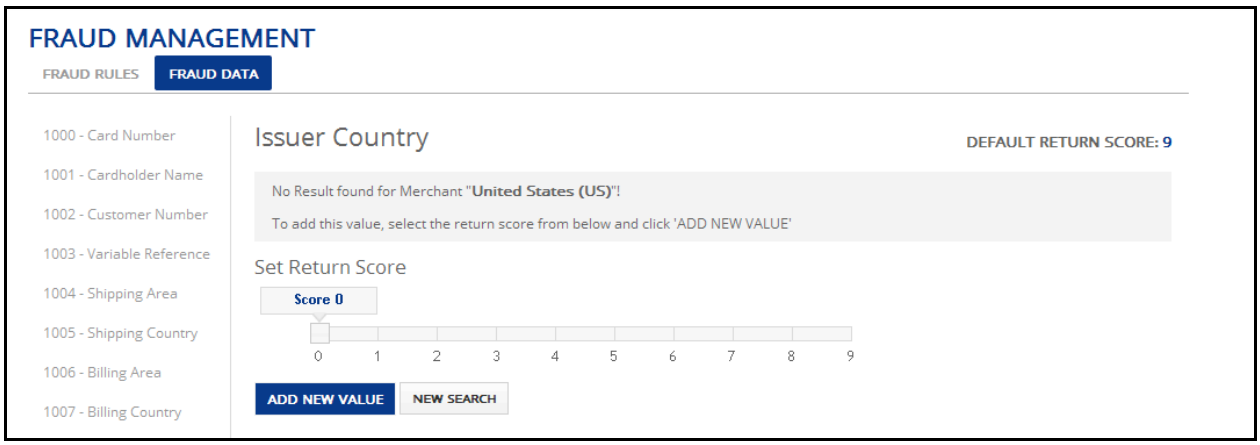
Note: A score of 9 is automatically assigned as the default return score.

Examples of Configuring Zone 1000 rules

Example 1

“Rule 1010 - Issuer country" can be set up to return a low score if the card number used in the transaction is of a specific issuing country (in this example we will use US – UNITED STATES). The default score can be set up to return a high score for all other countries. In this way, certain countries can be set up as high risk countries.

1. Login to Reporting, click **Fraud Management** and then **Fraud Data**.
2. In the Fraud Data screen, choose the rule that you wish to configure (for this example, “1010 – Issuer Country”).
3. Select “United States (US)” - the value that we wish to check for – from the dropdown and click **Go**. The following will be displayed:



4. Select a number from 0-9 on the scale; this is the score that will be returned if the Issuer Country of the card used for the transaction is the US. Fraud Management works on the basis that the lower the score, the higher the potential for fraud so the higher risk you consider this country to be, the lower the score that you should assign to it.
5. Click **Add New Value.**

Note: At this point, this issuer country has been added to the list of values for this rule but the rule itself is not yet enabled. Rule activation is described in Setting up the TSS Option in Section 4.1. If the rule is not enabled, no score will be returned for the rule and the rule will have no bearing on the overall transaction score.

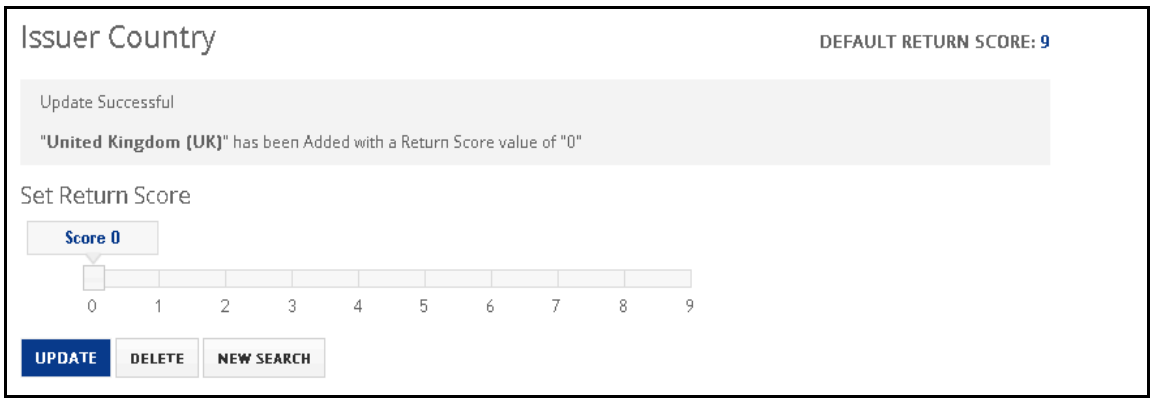
Example 2

"Rule 1010 - Issuer country" can be used in reverse to flag any issuer country other than a specified country (or countries) as high risk. This is implemented by assigning a high score to the country in question (in this example, "United Kingdom – UK") and selecting a low score as the default score. Then, if the issuer country for a transaction is the United Kingdom, a high score will be returned and a low score will be returned for all other issuer countries. In this way, the presence of UK as the issuer country is an indicator that the rule has "passed" and any other issuer country is an indicator that the rule has "failed".

1. Login to Reporting, click on **Fraud Management**.
2. In the **Fraud Data** section, select the rule that you wish to configure (for this example, "1010 – Issuer Country").
3. Select "United Kingdom (UK)" - the value that we wish to check for – from the dropdown and click **Go**.

4. Select a number from 0-9 on the scale; this is the score that will be returned if the issuer country of the card used for the transaction is the UK. Fraud Management works on the basis that the higher the score, the lower the potential for fraud, so the lower risk you consider this country to be, the higher the score should be. Typically 9 would be used to indicate that the rule has been passed.

5. Click **Add New Value.**



6. Now you must set the default score that will be returned for all other issuer countries. Click on the **Update** button beside "Default Return Score". We wish to return a low score if the Issuer Country is anything other than United Kingdom. Typically 0 would be used to indicate that the rule has failed. **Click Update.**

7. Now if we receive a transaction with a card issuer country other than United Kingdom, the rule will return a 0.

Note: At this point, this issuer country has been added to the list of values for this rule and the default value has been set but the rule itself is not yet enabled. Rule activation is described in Setting up the TSS Option in Section 4.1. If the rule is not enabled, no score will be returned for the rule and the rule will have no bearing on the overall transaction score.

3.2.2 Zone 2000

The checks in Zone 2000 compare certain fields in the transaction against other fields in the transaction to check if there is any conflict that might indicate fraud. For example, if the billing country and shipping country are different, this would potentially flag an issue as it may suggest that the customer is living in a different country than the address the card is registered at. These checks are common to all merchants in that they do not require any specific data from the merchant (unlike the majority of the Zone 1000 checks). Another difference between these checks and the Zone 1000

checks is that the merchant does not assign scores to the various scenarios that may arise; in general the zone 2000 checks can either pass or fail and as such, the only scores that can be returned are 9 to indicate failure and 0 to indicate a pass (although for some checks, there is a third scenario in which a score of 5 is returned; this will be described below).

The merchant does not need to enter information in the Fraud Data section for these rules; the rules just need to be as described in "Setting up the TSS Option".

Zone 2000 Data Sanity Checking for all Merchants.

Code	Title	Description
2000	Even amount.	If the transaction amount is an even amount, then this rule will fail. The pass score is 9 and the fail score is 0.
2001	Shipping and Billing countries.	This rule compares the shipping country to the billing country in the TSS and/or Auth request. If they are the same the rule will pass; if they differ the rule will fail. The pass score is 9 and the fail score is 0.
2002	Card Issuer country to Shipping country.	This rule compares the card issuer country (as returned by Elavon Payment Gateway) to the shipping country sent in the TSS and/or Auth request. If they are the same, the rule will pass; if they differ, the rule will fail. The pass score is 9 and the fail score is 0. If Elavon Payment Gateway do not have a record of the card issuer's country, then a score of 5 is returned to signify that the countries may be the same. Please note that this rule works with credit cards - ROI should be assumed as the issuer country for Laser and UK for Switch. AMEX cards will always return 5.
2003	Card Issuer country to Billing country.	This rule compares the card issuer country (as returned by Elavon Payment Gateway) to the billing country sent in the TSS and/or Auth request. If they are the same the rule will pass; if they differ, the rule will fail. The pass score is 9 and the fail score is 0. If Elavon Payment Gateway do not have a record of the card issuer's country, then a score of 5 is returned to signify that the countries may be the same Please note that this (and the next) rule works with credit cards - ROI should be assumed for Laser and UK for Switch. AMEX cards will always return a five.

Code	Title	Description
2004	Card issuer country to home country.	This rule compares the card issuer country (as returned by Elavon Payment Gateway) to the merchant's home country (as determined by the customer's IP address). If they are the same, the rule will pass; if they differ, the rule will fail. The pass score is 9 and the fail score is 0. If Elavon Payment Gateway do not have a record of the card issuer's country, then a 5 is returned to signify that the countries may be the same. Please note that this is a credit card issuer rule - Laser and Switch cards are assumed to be issued by ROI and UK institutions respectively and AMEX are not included in this rule.

3.2.3 Zone 3000

The checks in Zone 3000 compare data in a transaction against data from previous transactions. Some of these checks may require additional input from the merchant in the form of setting parameters.

Zone 3000 checks use historical data from transactions that the merchant has previously processed to assess the fraud potential of the current transaction. For some rules, certain parameters must be set by the merchant in order to determine the data that these rules will use (see Parameters section). The previous transactions that are used to establish patterns are from all accounts unless it is specifically stated that it is account specific.

Zone 3000 Data Pattern Checking

Code	Title	Description
3100	Same card used with different name.	This rule checks to see if the cardnumber used in the transaction has been used with a different cardholder name. The score will be lower depending on the number of times that the card has been used with a different name: 9 - If the cardnumber has not been used with another cardholder name other than the cardholder name provided in the current transaction. 8 - If the cardnumber has been used with two different cardholder names. This includes the current transaction (i.e. 8 will be returned if the cardnumber has been used in one transaction, other than the current transaction, with a different cardholder name than that provided in the current transaction). 7 - Three cardholder names. 6 - Four cardholder names. 5 - Five cardholder names. ….. 0 - Ten or more cardholder names.
3101	Same card used with different customer number.	This rule checks to see if the cardnumber used in the transaction has been used with a different Customer Number. The score will be lower depending on the number of times that the card has been used with a different Customer Number: 9 - If the cardnumber has not been used with another Customer Number other than the Customer Number provided in the current transaction. 8 - If the cardnumber has been used with two different Customer Numbers. This includes the current transaction (i.e. 8 will be returned if the cardnumber has been used in one transaction other than the current transaction with a different Customer Number than that provided in the current transaction). 7 - Three Customer Numbers. … 1 – Nine Customer Numbers. 0 - Ten or more Customer Numbers.

Code	Title	Description
3102	Same card used with different variable reference.	This rule checks to see if the cardnumber used in the transaction has been used with a different Variable Reference: The score will be lower depending on the number of times that the card has been used with a Variable Reference: 9 - If the cardnumber has not been used with another Variable Reference other than the Variable Reference provided in the current transaction. 8 - If the cardnumber has been used with two different Variable References. This includes the current transaction (i.e. 8 will be returned if the cardnumber has been used in one transaction other than the current transaction with a different Variable Reference than that provided in the current transaction). … 1 – Nine Variable References. 0 - Ten or more Variable References.
3103	Same card used with different variable reference in past 24 hours.	This rule checks to see if the cardnumber used in the transaction has been used with a different Variable Reference in the last 24 hours The score will be lower depending on the number of times that the card has been used with a different Variable Reference: 9 - If the cardnumber has not been used with another Variable Reference (within the last 24 hours) other than the Variable Reference provided in the current transaction 8 - If the cardnumber has been used with two different Variable References. This includes the current transaction (i.e. 8 will be returned if the cardnumber has been used in one transaction, other than the current transaction, with a different Variable Reference than that provided in the current transaction). … 1 – Nine Variable References. 0 - Ten or more Variable References.

Code	Title	Description
3200	Customer number used with different Card.	This rules checks to see if the Customer Number used in the transaction has been used with a different cardnumber. The score will be lower depending on the number of times that the Customer Number has been used with a different cardnumber: 9 - If the Customer Number has not been used with another cardnumber other than the cardnumber provided in the current transaction. 8 - If the Customer Number has been used with two different cardnumbers. This includes the current transaction (i.e. 8 will be returned if the Customer Number has been used in one transaction, other than the current transaction, with a different cardnumber than that provided in the current transaction). … 1 – Nine cardnumbers. 0 - Ten or more cardnumbers.
3201	Variable reference used with different Card.	This rules checks to see if the Variable Reference used in the transaction has been used with a different cardnumber. The score will be lower depending on the number of times that the Variable Reference has been used with a different cardnumber: 9 - If the Variable Reference has not been used with another cardnumber other than the cardnumber provided in the current transaction 8 - If the Variable Reference has been used with two different cardnumbers. This includes the current transaction (i.e. 8 will be returned if the Variable Reference has been used in one transaction, other than the current transaction, with a different cardnumber than that provided in the current transaction). … 1 – Nine cardnumbers. 0 - Ten or more cardnumbers.

Code	Title	Description
3202	Customer Name used with different card.	This rules checks to see if the cardholder name used in the transaction has been used with a different cardnumber. The score will be lower depending on the number of times that the cardholder name has been used with a different cardnumber: 9 - If the cardholder name has not been used with another cardnumber other than the cardnumber provided in the current transaction. 8 - If the cardholder name has been used with two different cardnumbers. This includes the current transaction (i.e. 8 will be returned if the cardholder name has been used in one transaction, other than the current transaction, with a different cardnumber than that provided in the current transaction). … 1 – Nine cardnumbers. 0 - Ten or more cardnumbers.
3203	Variable reference used with a different card in past 24 hours.	This rule checks to see if the Variable Reference used in the transaction has been used with a different cardnumber in the last 24 hours. The score will be lower depending on the number of times that the Variable Reference has been used with a different cardnumber: 9 - If the Variable Reference has not been used with another cardnumber (within the last 24 hours) other than the cardnumber provided in the current transaction. 8 - If the Variable Reference has been used with two different cardnumbers. This includes the current transaction (i.e. 8 will be returned if the Variable Reference has been used in one transaction, other than the current transaction, with a different cardnumber than that provided in the current transaction). … 1 – Nine cardnumbers 0 - Ten or more cardnumbers
3300	Repeat Customer.	Returns 9 if there is a previous transaction with the same Variable Reference, Customer Number, card number and cardholder name. Otherwise 0 will be returned.

Code	Title	Description
3301	Number of times card authorised in past 24 hours.	Returns a score that indicates the number of times this card has been authorised on the account in the past 24 hours. The score will be lower depending on the number of times that the card has been authorised. 9 – Once. 8 – Twice. … 0 - Ten times or more.
3302	Number of times card authorised in past week.	Returns a score that indicates the number of times this card has been authorised in the past week. The score will be lower depending on the number of times that the card has been authorised. 9 – Once. 8 – Twice. … 0 – Ten times or more.
3303	Number of times card used in past 24 hours.	Returns a score that indicates the number of times this card has been used (authorisation attempted) in the past 24 hours. The score will be lower depending on the number of times that the card has been used. 9 – Once. 8 – Twice. … 0 – Ten times or more.
3304	Number of times used in past week.	Returns a score that indicates the number of times this card has been used (authorisation attempted) in the past week. The score will be lower depending on the number of times that the card has been used. 9 – Once. 8 – Twice. … 0 – Ten times or more.
3305	Number of times Variable reference used in past 24 hours.	Returns a value to determine the number of times this variable reference has been used in the past week. The score will be lower depending on the number of times that the Variable Reference has been used. 9 – Once. 8 – Twice. … 0 – Ten times or more.

3.2.4 Zone 5000

The Zone 5000 rules are based on checks that occur during authorisation, e.g. the address check and security code check.

Note: Because the results of these checks are not known until the response from the bank is received, the scores from these rules cannot be calculated until after the authorisation. This means that these checks cannot be used for TSS Autocheck (as Autocheck declines the transaction before authorisation). Similarly, if you are using the TSS transaction to determine the Fraud Score before authorisation, the results of these rules will not be known at this time and the overall Fraud Score may be altered after the authorisation depending on the results of these rules.

Code	Title	Description
5001	Check AVS Postcode Response (Account Specific)	The score is based on the AVS (Address Verification Service) check performed by the customer's issuing bank on the digits from the **post code** of the billing address. The score depends on the AVS Postcode result: N (Not Matched)- 0 P (Partial Match - 5 M (Matched) - 9 U (Unable to check – not certified etc) - 9 I (Problem with check) - 9
5002	Check AVS Address Response (Account Specific)	The score is based on the AVS (Address Verification Service) check performed by the issuing bank on the digits from the **street address** of the billing address. The score depends on the AVS Address result: N (Not Matched) - 0 P (Partial Match) - 5 M (Matched) - 9 U (Unable to check – not certified etc) - 9 I (Problem with check) - 9
5003	Check CVN result Response (Account Specific)	The score is based on the check performed by the issuing bank on the Security Code (CVN) of the customer's card. The score depends on the Security Code Result: N (CVN Not Matched) - 0 M (CVN Matched) - 9 U (CVN Not Checked – issuer not certified) - 9

4 Setting up Fraud Management Rules

This chapter describes the configuration of the Fraud Management rules.

4.1 Setting up Fraud Management Rules

4.1.1 Setting up the TSS Option

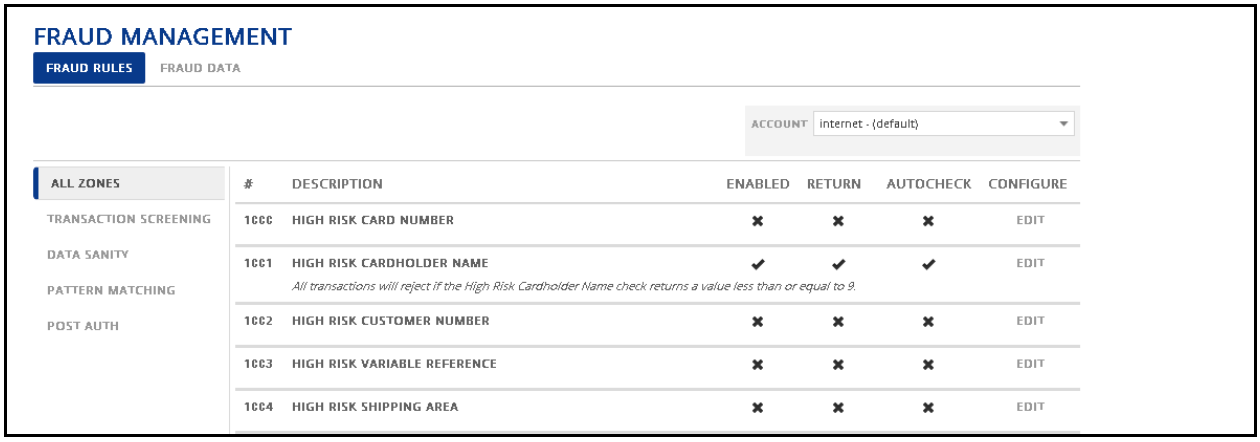
The TSS (Transaction Suitability Scoring) option allows merchants to score their transactions without declining them. This is set up as follows:

Set up in Reporting:

As described above there are 4 types of rules - Zones 1000, 2000, 3000 and 5000. All rules are configured in the Fraud Rules section but most Zone 1000 rules (specifically rules 1002 – 1011 and rule 1013) also require extra configuration on the Fraud Data screen (as described in section 3.2).

The Fraud Rules Screen:

When you click into the Fraud Rules screen, you will be presented with a list of all Fraud Management Rules. On the left of the screen, you can click on a zone to show only the rules for that zone.



The columns on the right specify if each rule is “Enabled” and set up for “Return” and “Autocheck”. “Enabled” means that the rule is activated and will have a bearing on the overall score for the transaction. “Return” means that the individual score for this rule will be returned in the transaction response and displayed in Reporting. “Autocheck” means that transactions may be automatically declined on the basis of this rule. “Edit” may be clicked in the “Configuration” column for each rule in order to change these values (and to perform further configuration on the rule).

Note: Fraud Management rules are enabled per sub-account. On the top right, of the screen, there is an "Account" dropdown menu. If you have multiple sub-accounts on your account, ensure that the correct sub-account is selected before you configure your rules. When you select a sub-account name in the dropdown, the "Enabled" "Return" and "Autocheck" status shown for each rule will pertain to this sub-account. For more information on sub-accounts, please see the *Elavon Auth Developer's Guide*.

Enabling the Rule:

For a rule to return a Fraud Score, it must first be enabled.

To enable a rule:

- Go to the **Fraud Rules** section.
- Click on the **Edit** button to the right of the check that you wish to enable.
- Set the **Check Enable/Disable** button to "On".
- Click **Update**.

Setting up the Weight:

Every rule that is set up must have a weight. The importance of each rule can be specified using its weight; the higher the weight the more important the rule. If a rule has a higher weight, it will have more influence on the overall score (for more information on the calculation of the overall score, please see section 5.1).

To set up the weight:

- Go to the **Fraud Rules** section.
- Click on the **Edit** button to the right of the check that you wish to assign a weight to.
- Click on the "**+**" symbol beside **Advanced** and enter the required weight in the text box.
- To equally weight the rules, set all weights to the same value. To set a rule to a higher importance, increase its weight.
- Click **Update**.

Setting up the Response Values:

Every rule that is set up must have its **Return Value In Response** button set to **On**. When this button is set to **On**, the score for the rule will be returned in the transaction response and will also be displayed in the transaction details in Reporting.

To enable the response value:

- Go to the **Fraud Rules** section.
- Click on the **Edit** button to the right of the rule that you wish to configure.
- Set **Return Value In Response** to **On.**
- Click **Update**.

4.1.2 Setting up the TSS with Autocheck Option

TSS Autocheck is a method by which transactions can be automatically rejected based on the Fraud Score results. This means that transactions that are suspect according to the merchant's Fraud Management configuration can be blocked automatically before they are authorised.

For TSS with autocheck, the Fraud Management rules must be set up as for the TSS option; however additional rejection rules must also be configured in order to specify when the transaction should be rejected. Because Autocheck rejects transactions that may have otherwise been authorised by the bank, **it is very important that the Fraud Management settings are configured correctly before adding rejection rules** to ensure that transactions will be declined only as intended.

Setting up TSS Autocheck:

The rejection rules are simply an extension of the Zone 1000, 2000 and 3000 rules so in order to set up rejection rules, the configuration described in "Setting up the TSS Option" is also necessary.

Setting up Fraud Management rejection rules.

Within the section "Fraud Rules" the merchant can specify that a transaction should reject if it breaks a certain rule.

Reject based on a specific check.

Within the "Fraud Rules" section, a rejection rule can be set up for the individual rules. In order to set up these fraud rules in accordance with your requirements, it is very important to understand the way in which the scores are calculated for the rules in question. For more information on this please see Section 3 of this guide.

To reject a transaction that fails an individual rule:

- Click **Fraud Rules** in the Fraud Mangement section.
- Click the **Edit** button to the right of the rule that you wish to configure.
- Set the **Autocheck Enable/Disable** button to "On". The rejection rule will appear. In the case where the rule can only return a score of 9 or 0 (i.e. pass or fail), no further configuration is needed. In the case of those 2000 checks for which the issuer country is compared to the shipping/billing/home country, it will be necessary to specify if the transaction should be rejected if the issuer country is unknown. In the case of those checks for which various scores can be returned, you will need to select the condition ("less than", "less than or equal to", "greater than", "equal to or greater than" or "equals") and the score.
- Click the **Update** button.

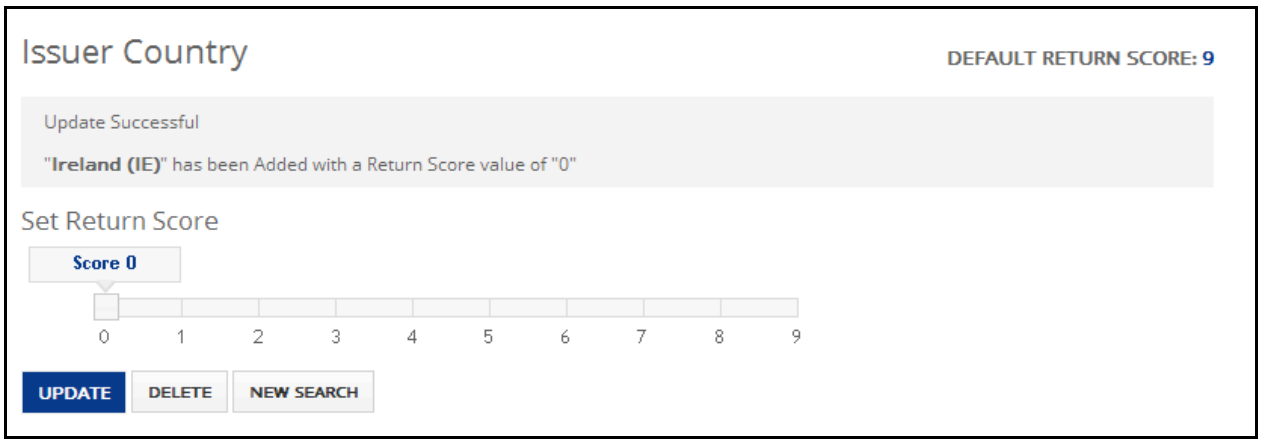
A sample configuration of a Fraud Management rule with a Rejection Rule is outlined below.

Scenario

The merchant only wants to accept transactions from Irish issued cards as they can only ship products within Ireland. They want to decline transactions where the card is issued in any other country.

First set up the fraud data:

1. On the "Fraud Data" screen select the **1010: Issuer Country** rule. Choose "Ireland (IE)" from the drop-down menu. Click **Go.**
2. Set the return score to 9 on the scale. Click **Add New Value.** Now if the issuing country is Ireland, a score of 9 will be returned for this rule.



3. Click Update beside “Default Return Score” on the “Fraud Data” screen.
4. Set the default return score to 0 on the scale. Click **Add New Value**. Now if the issuing country is not Ireland, a score of 0 will be returned for this rule.

Then you must enable the rule:

- Go to the **Fraud Rules** screen.
- Click on the **Edit** button for the check 1010 “High Risk Issuer Country”
- Set the **Check Enable/Disable** button to “On”.
- Set the Return Value in Response to “On” so that the result of the rule will be returned in the response and displayed in Reporting.

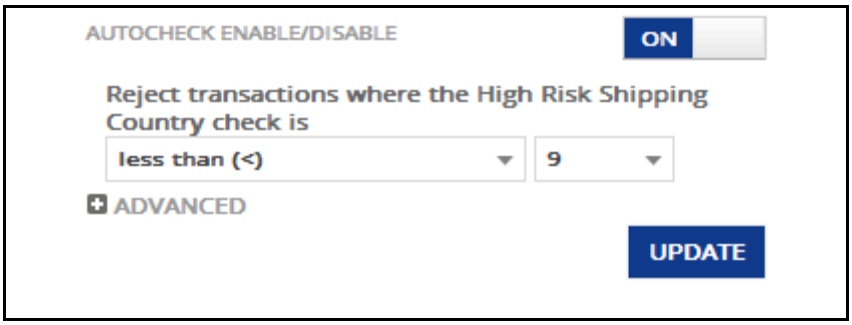
Setting up the weight.

A weight must be set for all checks that will be used.

Set the weight of check "1010 High risk issuer country". See previous section, **Setting up the weight.**

Finally you must configure the rejection rule:

- Set **Autocheck enabled/disable** to “On”
- Select “less than (<)” from the “Select Rule” dropdown and select 9 from the score dropdown. In this way, any transaction that scores less than 9 for this rule will be rejected.



As every country other than IE will return a 0 for this rule, all countries except IE will be rejected with a result code of 107.

5 Calculating the Fraud Score

5.1 Calculating the Overall Fraud Score

The overall score is made up of the sum of the individual weighted scores from each. The weighted score for a rule is calculated as follows:

$$\left\{ \frac{(N+1) * \text{weight}}{\text{Total weight}} \right\} *$$

Where:

N = the rule's result.

weight = the rule's weight.

Total weight = The summed weight of all activated rules.

Examples

5.2.1 Scenario 1

Only 1 rule is set up, Rule 1010 is set up to return a 9 if it passes and 0 if it fails. It is weighted as 100.

If the rule passes, the score will be:

Check 1010 calculation

$$\frac{[(9+1) * 100] * 10}{100}$$

$$= \frac{[1000] * 10}{100}$$

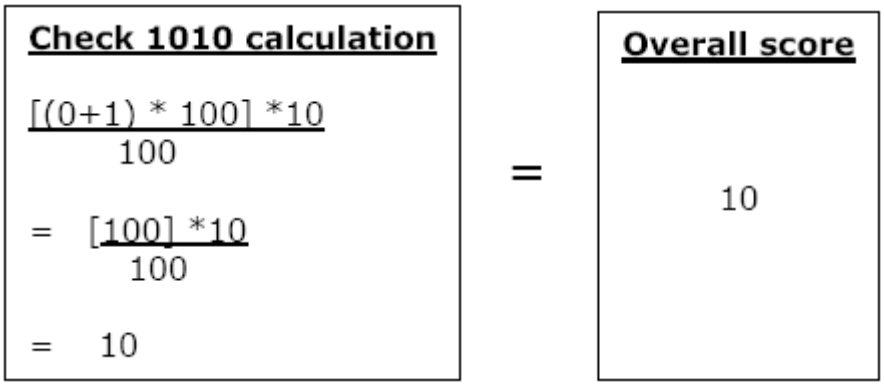
$$= 100$$

=

Overall score

100

If the rule fails, the score will be:

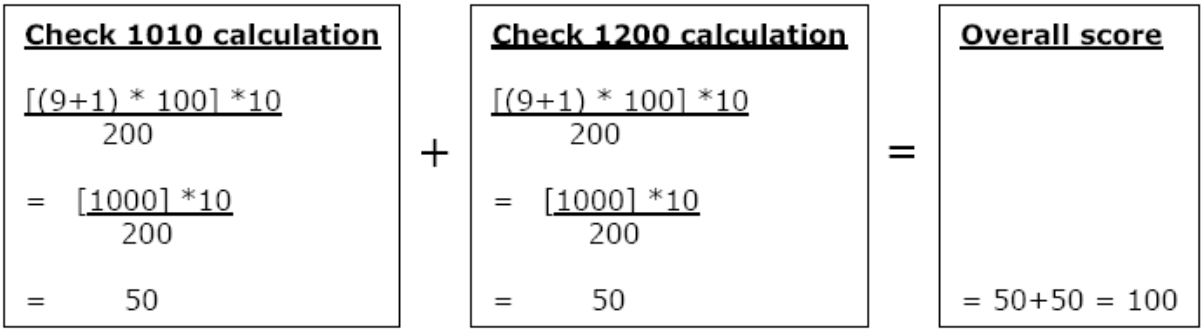


5.2.2 Scenario 2

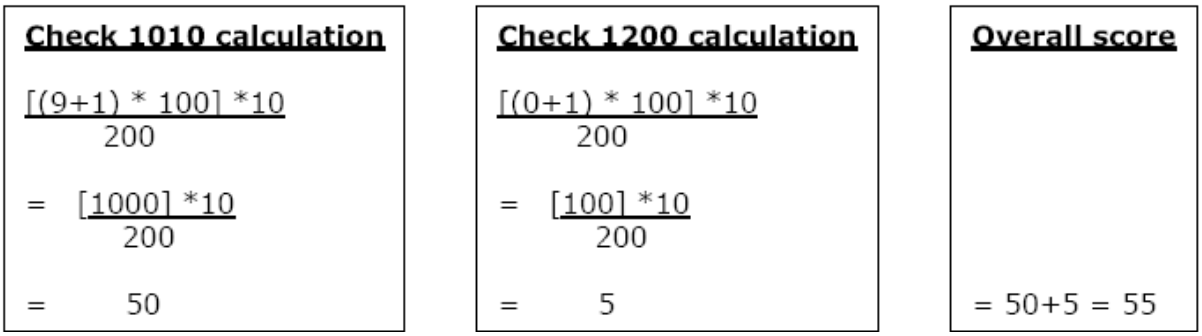
2 rules are set up with equal weights - rule 1010 is set up to return a 9 if it passes and 4 if it fails.

Rule 1200 is set up to return a 9 if it passes and 0 if it fails. Both have a weight of 100.

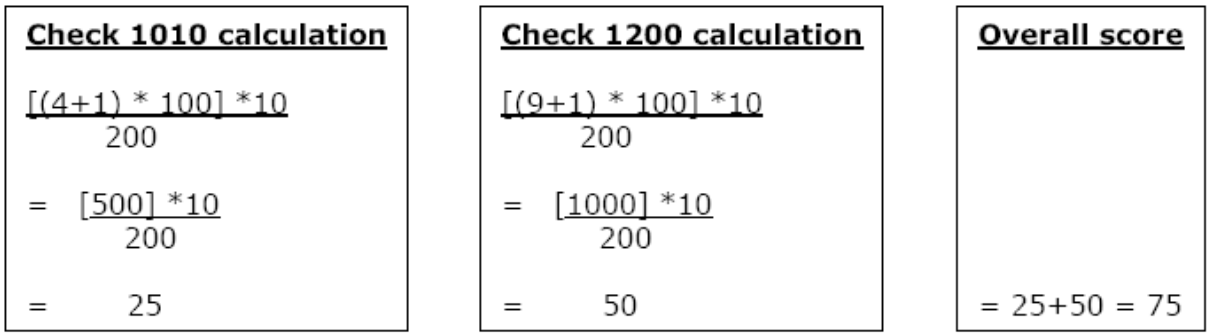
If the rule 1010 passes and rule 1200, passes the score will be:



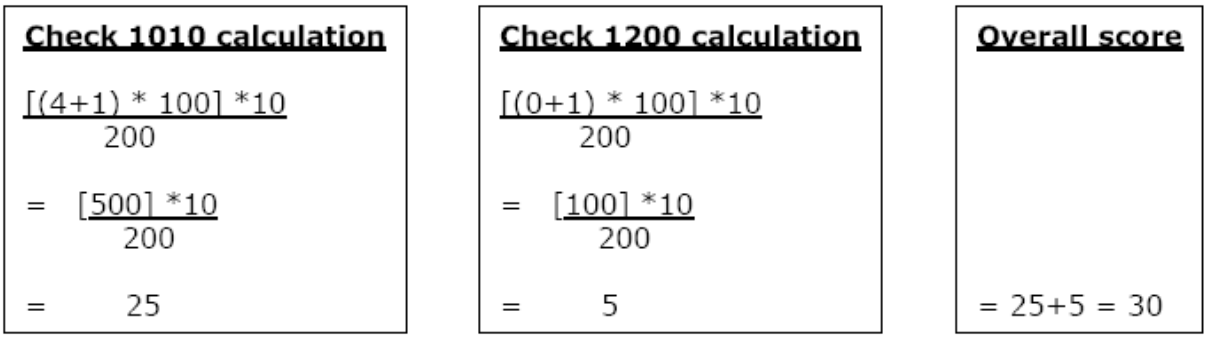
If the rule 1010 passes and rule 1200 fails, the score will be:



If the rule 1010 fails and rule 1200 passes, the score will be:



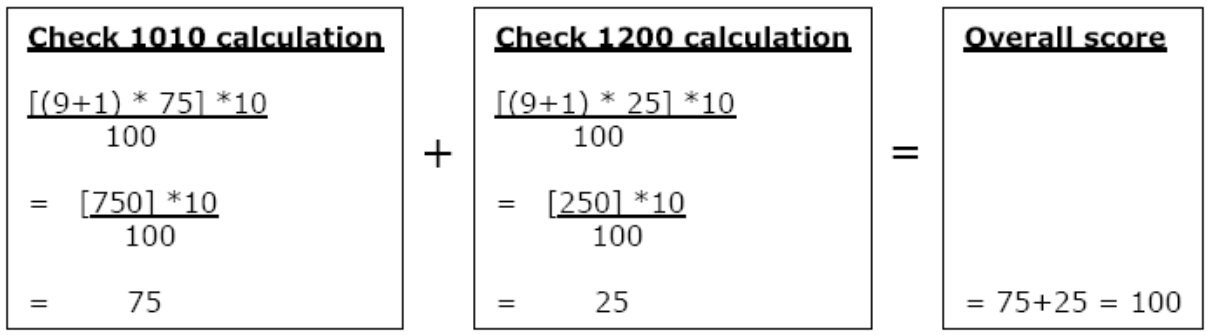
If the rule 1010 fails and rule 1200 fails, the score will be:



5.2.3 Scenario 3

2 rules are set up with different weights- rule 1010 is set up to return a 9 if it passes and 4 if it fails and has a weight of 75. Rule 1200 is set up to return a 9 if it passes and 0 if it fails and has a weight of 25.

If the rule 1010 passes and rule 1200 passes, the score will be:



If the rule 1010 passes and rule 1200 fails, the score will be:

Check 1010 calculation	Check 1200 calculation	Overall score
$\frac{[(9+1) * 75] * 10}{100}$ $= \frac{[750] * 10}{100}$ $= 75$	$\frac{[(0+1) * 25] * 10}{100}$ $= \frac{[25] * 10}{100}$ $= 2.5$	= 75+2.5 = 77.5

If the rule 1010 fails and rule 1200 passes, the score will be:

Check 1010 calculation	Check 1200 calculation	Overall score
$\frac{[(4+1) * 75] * 10}{100}$ $= \frac{[375] * 10}{100}$ $= 37.5$	$\frac{[(9+1) * 25] * 10}{100}$ $= \frac{[250] * 10}{100}$ $= 25$	= 37.5+25 = 62.5

If the rule 1010 fails and rule 1200 fails, the score will be:

Check 1010 calculation	Check 1200 calculation	Overall score
$\frac{[(4+1) * 75] * 10}{100}$ $= \frac{[375] * 10}{100}$ $= 37.5$	$\frac{[(0+1) * 25] * 10}{100}$ $= \frac{[25] * 10}{100}$ $= 2.5$	= 37.5+2.5 = 40