secure trading
ONLINE PAYMENT EXPERTS

Fraud Checks

Published: 5 June 2019

Table of Contents

1 Introduction 3

2 Reason codes 4

3 Fraud rating 5

4 Managing transactions 6

4.1 Viewing fraud rating and reason codes in MyST 6
4.2 Settle status 7

5 Negative Database 9

6 Additional Notes 10

6.1 Email warnings 10
6.2 Confidence threshold 11
6.3 Duplicate checks 11
6.4 AVS & CVV2 Checks 12
6.5 3-D Secure 13

7 Further Information and Support 14

7.1 Secure Trading Support 14
7.2 Secure Trading Sales 14
7.3 Useful Documents 14
7.4 Frequently Asked Questions 14

1 Introduction

The internal fraud check service provided by Secure Trading analyses authorised transactions for attributes that may be considered suspicious, prior to settlement being performed.
These checks are performed at pre-defined times throughout the day.

When fraud checks are enabled, transactions suspected of being fraudulent are automatically suspended, deferring their settlement until you take action. This allows you to manually inspect and manage suspicious transactions processed on your account.

Fraud checks are disabled by default on all new site references.
To enable fraud checks on your account, please contact Secure Trading Support (see section 7.1).

Secure Trading cannot guarantee to identify all fraudulent transactions.

2 Reason codes

Secure Trading performs the following checks on authorised transactions in settle status “0” against records for the previous 7 days. If any of the following criteria are met, the fraud rating for the transaction will be incremented by the number shown on the right. A higher fraud rating indicates a greater chance of fraud, and as such transactions with high fraud ratings may be suspended (see section 3 for further information).

The following checks are performed on each transaction prior to settlement:

All reason codes		
X	The same card number has been previously declined with different expiry dates.	+1
E	The billing email address has been used with different declined cards / expiry dates / issue numbers.	+1
N	Cardholder name has been used with different declined cards / expiry dates.	+1
C	The customer has processed an unusually large number of successful transactions on your site using the same card details.	+1
V	The cardholder name contains repeated letters or punctuation, leading us to believe invalid names have been used. (e.g. “ghghghghg”).	+1
P	The postcode did not match that on the customer’s bank’s records.	+1
S	The security code did not match that on the customer’s card.	+2
G	The card number or billing address submitted has been found in the negative database.	+10

The character on the left represents what we call the **reason code**. Following fraud checks, you can view which of the checks failed (if any), by matching the resulting reason codes with the list above.

The number on the right indicates by how much Secure Trading will increment a transaction’s fraud rating if the criteria are met.

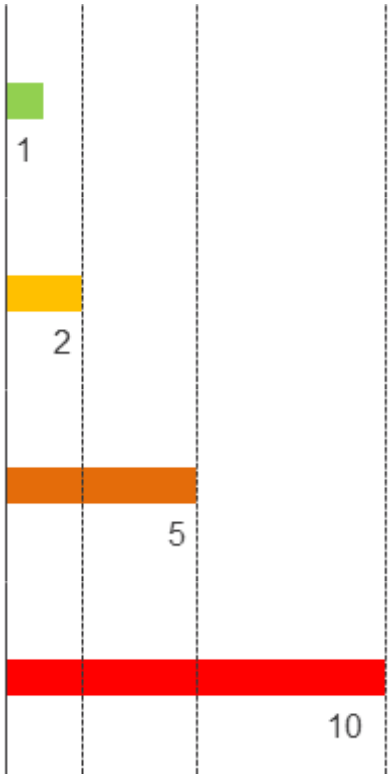
3 Fraud rating

The fraud rating is used to indicate how suspicious a transaction is, based on a number of criteria. These criteria are described in greater detail in section 2.

Before the fraud checks have been run, the fraud rating will be -1.

Following the processing of the fraud checks, a fraud rating of 0 indicates that nothing suspicious was discovered by our fraud checks.

Every suspicious attribute found by the fraud checks will increment the fraud rating. A higher fraud rating indicates a more suspicious transaction.



Low fraud rating

When the fraud rating is 0 or 1, the transaction will be regarded by STPP as legitimate and will trigger no warnings.

Email warning sent

When the fraud rating reaches 2, it will trigger a warning regarding the transaction to be emailed to the address associated with your ST account.

Confidence threshold reached

When the fraud rating reaches 5, Secure Trading will suspend the transaction and automatically confirm this via email.
The confidence threshold can be customised on your sites (see section 6.2).

Updating negative database

When the fraud rating reaches 10, Secure Trading will record the details of the card and billing email in their internal negative database. For further information on the negative database (see section 5).

Example

e.g. If the security code did not match the customer's card and the card number was also in our negative database:

- The fraud rating would be 12 (+2 for the security code and +10 for the negative database).
- The reason codes listed would be S and G.
- [Providing the confidence threshold is 5, as is default] The transaction will be automatically suspended.

Because the fraud rating is higher than 10, the customer's email address will be added to Secure Trading's internal negative database. Future transactions using this email address will cause 10 to be added to their fraud ratings.

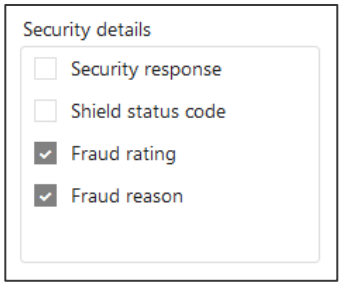
4 Managing transactions

4.1 Viewing fraud rating and reason codes in MyST

You can view the fraud rating and reason codes (if any) for each transaction in MyST.
(See our MyST documentation for info on viewing transactions)

4.1.1 Transaction Search

Select “Fraud rating” and “Fraud reason” in the optional “**Fields**” tab when performing a search on the “**Transaction Search**” page.

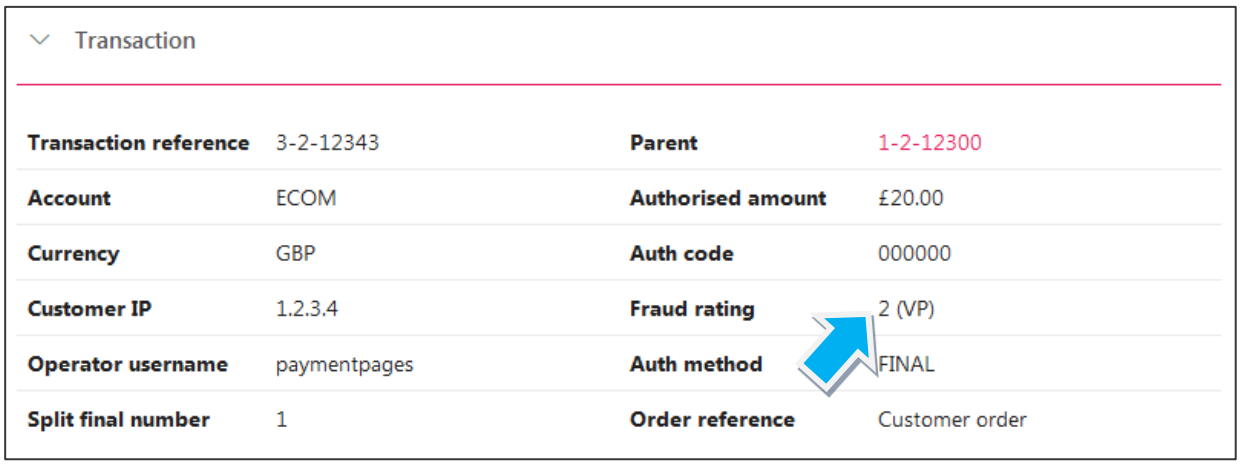


This allows you to compare fraud ratings/reasons of multiple transactions that meet your search criteria.

Reference	Status	Account	Request	Payment	Timestamp	Settle amount	Fraud rating	Fraud reason
1-2-12345	Suspended	ECOM	AUTH		2019-05-19 09:28:51	£51.20	2	S
1-2-12344	Suspended	ECOM	AUTH	VISA Debit	2019-05-19 09:28:45	£58.45	10	G
3-2-12343	Pending	ECOM	AUTH	VISA Debit	2019-05-19 09:28:36	£34.00	2	VP
1-2-12342	Suspended	ECOM	AUTH	VISA Debit	2019-05-19 09:28:32	£16.99	3	SP
2-2-12341	Pending	ECOM	AUTH	VISA Debit	2019-05-19 09:28:17	£11.00	0	

4.1.2 Single Transaction View

The fraud rating and reason(s) are also visible in the single transaction view, as shown below.



4.2 Settle status

All Secure Trading transactions are assigned a settle status:

Settle status	Description
0	Awaiting settlement. If this transaction passes the fraud checks, it will be settled. (Checks only run if enabled)
1	Fraud checks have been overridden and will not be run on this transaction. Transaction will be allowed to settle.
2	Transaction has been suspended. This is temporary state that will allow you to delay settlement for up to 7 days.
3	Transaction has been permanently cancelled. It can no longer be settled.
100	Transaction has been settled successfully.

4.2.1 Updating the settle status

Sign in to MyST, search for the transaction and click "**Update**". Modify the settle status of the transaction and click "**Update**". (See our MyST documentation for info on updating transactions)
API users can perform a TRANSACTIONUPDATE XML Request.
(See **Transaction Update** document for further info on the API solution)

4.2.2 Allowing transactions to settle

If you have manually investigated a transaction that has been flagged with a particular fraud rating and would like to instruct STPP to settle the transaction, you can manually override a transaction by updating the settle status to 1.

Settlement is performed once a day and all transactions with settle status 1 are settled regardless of their fraud rating.

Please note that transactions with settle status 1 will still support the submission of other delayed settlement fields (such as the settle due date).

Secure Trading cannot take responsibility for potentially fraudulent transactions that have been manually overridden.

4.2.3 Suspending transactions

If you believe a transaction to be suspicious but it has not been automatically suspended, you can manually suspend a transaction by updating the settle status to 2.
Suspended transactions can later be re-enabled for settlement by updating the settle status to 1. They can also be permanently cancelled by updating the settle status to 3.

All payments not settled after 7 days from authorisation will be cancelled.

4.2.4

4.2.4 Cancelling transactions

If you have manually investigated a suspended transaction and would like to cancel the payment, you can manually cancel a transaction by updating the settle status to 3.

Cancelling a transaction is a permanent action.
Cancelled transactions can never be settled by Secure Trading.

5 Negative Database

Secure Trading's internal negative database is a record of card numbers and billing email addresses previously associated with suspicious transactions.

When any transaction receives a fraud rating of 10 or higher, STPP will automatically add the card number and billing email address to the database.

When a new transaction processed by any Secure Trading merchant includes a card number and/or billing email address that has been stored in the negative database, the fraud rating is increased by 10, which immediately suspends the transaction under default configuration. (This requires fraud checks to be enabled on your account)

If a transaction is suspended due to an entry in the negative database, it is shown with the reason code 'G' in MyST.

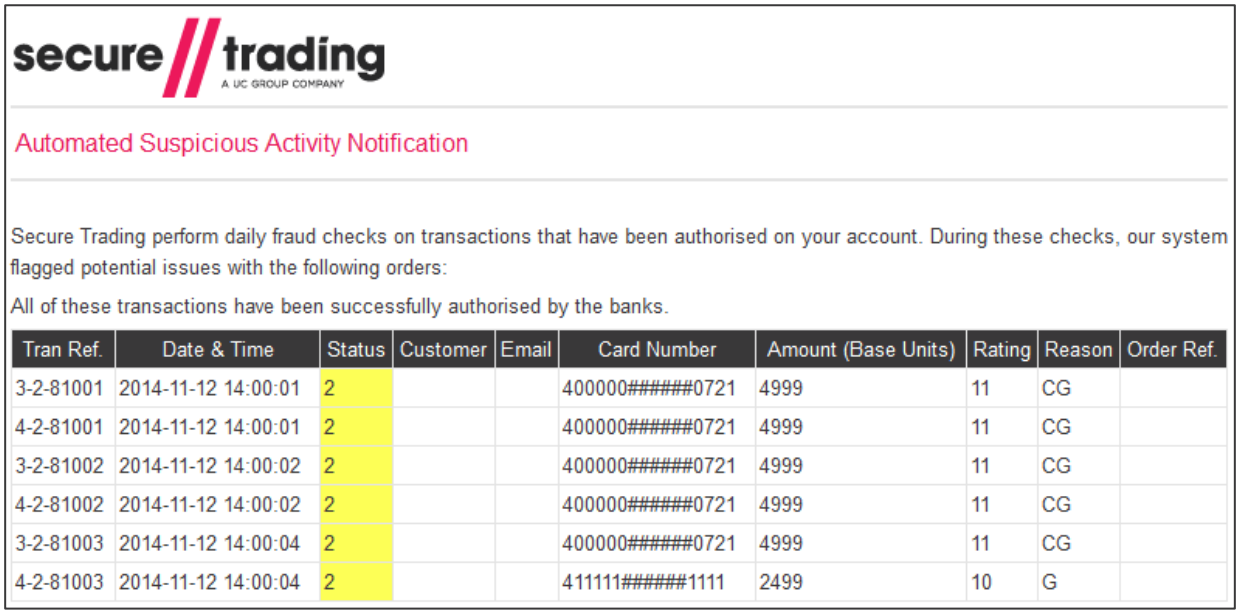
6 Additional Notes

6.1 Email warnings

Fraud email warnings are in HTML format and are sent from support@securetrading.com. Please ensure this sender is added to your whitelist.

Each email will contain a list of suspicious transactions (fraud rating of 2 or higher) for one of your sites (one email per site, per day).

It includes basic information on each transaction, including the fraud rating and reason the transaction was deemed suspicious (indicated by reason codes, see section 2).



secure trading
A UC GROUP COMPANY

Automated Suspicious Activity Notification

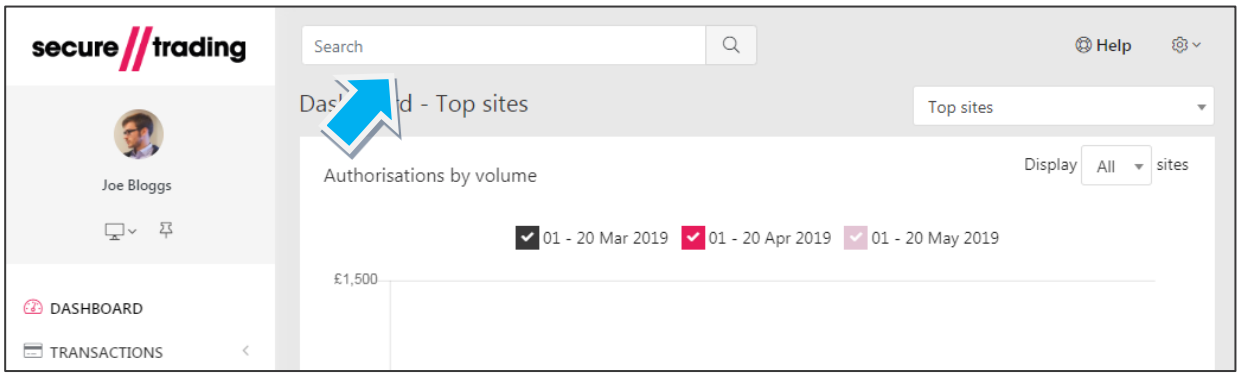
Secure Trading perform daily fraud checks on transactions that have been authorised on your account. During these checks, our system flagged potential issues with the following orders:

All of these transactions have been successfully authorised by the banks.

Tran Ref.	Date & Time	Status	Customer	Email	Card Number	Amount (Base Units)	Rating	Reason	Order Ref.
3-2-81001	2014-11-12 14:00:01	2			400000######0721	4999	11	CG	
4-2-81001	2014-11-12 14:00:01	2			400000######0721	4999	11	CG	
3-2-81002	2014-11-12 14:00:02	2			400000######0721	4999	11	CG	
4-2-81002	2014-11-12 14:00:02	2			400000######0721	4999	11	CG	
3-2-81003	2014-11-12 14:00:04	2			400000######0721	4999	11	CG	
4-2-81003	2014-11-12 14:00:04	2			411111######1111	2499	10	G	

Screenshot of fraud email warning

More information on each transaction can be found by signing in to MyST and typing the unique transaction reference into the universal search box at the top of the page (refer to our MyST documentation for further information).



6.2 Confidence threshold

By default, all transactions with a fraud rating of 5 are suspended by STPP following fraud checks. This is called the **confidence threshold** and it can be customised if required (e.g. suspend on fraud rating 9, instead). To do this, please contact Secure Trading Support and ask to change the confidence threshold for your site reference(s) (see section 7.1).

6.3 Duplicate checks

Secure Trading provides an additional service known as duplicate checks. When enabled on your account, duplicate checks suspend transactions that appear identical to previous transactions processed within the last 15 minutes. This is to automatically prevent assumed duplicate transactions (e.g. If the customer refreshes their browser and inadvertently sends two requests).

Please note that duplicate checks are performed independently of the aforementioned fraud checks. They are disabled by default on all new site references.

To enable duplicate checks on your account, please contact Secure Trading Support (see section 7.1).

6.4 AVS & CVV2 Checks

All UK banks support online address (AVS) and security code (CVV2) checks. These checks are automatically performed with each authorisation request if supported by the customer's bank.

More details on how AVS and CVV2 checks are performed can be found in the **AVS & CVV2 document**
All Secure Trading documents can be found on our website.

If the postcode and card security code (CVV2) don't match the records held by the customer's bank, the fraud rating is raised by 3 (+1 for invalid postcode and +2 for invalid CVV2)

6.4.1 Security Policy

The security policy on your account is independent of the fraud and duplicate checks and is enabled on all Secure Trading site references by default. The security policy will automatically suspend transactions (update to settle status 2) when the security code checks return a "not matched" response.

Please note that the security policy checks can be customised to suspend payments based on other criteria if required. Please contact Secure Trading Support (section 7.1) to specify criteria to be used to suspend your transactions.

6.4.2 Using rules

An alternative to using the security policy (see section 6.4.1) is to configure rules on your site reference. Rules are also independent of fraud and duplicate checks.

Rules and Payment Pages site security

If you are enabling Secure Trading Rules (starting with "STR-") for a Payment Pages solution, you must ensure you are using the latest version of site security, otherwise this could affect your service and the ability to process payments.

How to check if you are using the latest version:

- If the site security hash starts with the letter "g" you are using the new version.
- If the site security hash does not start with the letter "g" you are using the old version.

For info on the latest version of site security, refer to the **Payment Pages Setup Guide**.
If you are unsure, contact Support for further assistance (section 7.1).

When active, the *STR-1* rule will automatically cancel transactions (update settle status to 3) when the security code entered by the customer does not match the value held on the bank's records. This feature allows you to display a "Declined" message to your customer when the customer enters an incorrect security code.

For further information on configuring rules, please to our Rule manager documentation.

Please note that when a transaction is cancelled by a rule, the error code may remain in status "0" (Ok). This would indicate that the payment was authorised by the acquiring bank, but later cancelled by Secure Trading.

6.5 3-D Secure

3-D Secure is the collective term for Mastercard SecureCode and Verified by Visa.
It is an additional security measure provided free of charge by card issuers.
During payment, customers are directed to their card issuer's server where they verify their identity by entering a unique password and/or PIN known only to them.

Mastercard has mandated that all Maestro payments must use SecureCode. Merchants failing to follow this mandate may be liable to pay heavy fines.

Neither Mastercard SecureCode nor Verified by Visa (VbV) are mandatory (except for Maestro, see above), but they are recommended because in the event of a dispute with the transaction at a later date, the card issuer will usually take responsibility of the chargeback instead of the merchant.

3-D Secure is enabled on all new Secure Trading accounts by default, but you can disable this by contacting Secure Trading Support.

At the time of writing, Secure Trading only supports 3-D Secure for Mastercard and Visa-branded cards.

Merchants using API solutions will need to perform additional requests when performing 3-D Secure transactions. This process is described in-depth in the **3-D Secure** document

All Secure Trading documents can be found on our website.

Further information about Verified by Visa can be found at this URL:
http://www.visaeurope.com/making-payments/verified-by-visa/

Further information about Mastercard SecureCode can be found at this URL:
http://www.mastercard.us/merchants/securecode.html

7 Further Information and Support

This section provides useful information with regards to documentation and support for your Secure Trading solution.

7.1 Secure Trading Support

If you have any questions regarding integration or maintenance of the system, please contact our support team using one of the following methods.

Method	Details
Telephone	+44 (0) 1248 672 050
Fax	+44 (0) 1248 672 099
Email	support@securetrading.com
Website	http://www.securetrading.com/support/support.html

7.2 Secure Trading Sales

If you do not have an account with Secure Trading, please contact our Sales team and they will inform you of the benefits of a Secure Trading account.

Method	Details
Telephone	0800 028 9151
Telephone (Int'l)	+44 (0) 1248 672 070
Fax	+44 (0) 1248 672 079
Email	sales@securetrading.com
Website	http://www.securetrading.com

7.3 Useful Documents

The following documents should be read in conjunction with this document:

- STPP Web Services User Guide – This document describes how to process XML Requests and Responses through Secure Trading's Web Services solution.
- STPP XML Specification – This document details how to perform AUTH, REFUND and ACCOUNTCHECK XML Requests through Secure Trading.
- STPP Transaction Query – This document details how to perform TRANSACTIONQUERY XML Requests through Secure Trading.
- MyST documentation – This document outlines how to use the MyST interface.

Any other document regarding the STPP system can be found on Secure Trading's website (http://www.securetrading.com). Alternatively, please contact our support team as outlined above.

7.4 Frequently Asked Questions

Please visit the FAQ section on our website (http://www.securetrading.com/support/faq).