

eBook

# Fraud Prevention Guide



# Contents

<b>Introduction to Fraud Prevention</b>	<b>3</b>
<b>AVS/CV2</b>	<b>5</b>
<b>3D Secure and PSD2</b>	<b>13</b>
<b>Enhanced Fraud Screening</b>	<b>24</b>
<b>ACI Fraud Management</b>	<b>34</b>

# Introduction to Fraud Prevention

When processing any type of transaction, you always need to be aware of the potential risks of fraud, and what you can do to prevent it. In this guide we will look at the tools that are available to you to help with reducing the risk of fraud that your business is exposed to.

At Opayo, we make processing transactions as safe as possible, however we cannot offer any guarantees against fraudulent activity. By using the tools outlined in this guide, you will be able to make your own payments safer and more secure when processing CNP (Cardholder Not Present) transactions.

Any transaction that is processed either over the phone, on a website, or by mail order is classified as a CNP transaction. As the cardholder is not present when the transaction is being processed, Opayo have a number of tools you can use to limit the risk of fraud for your business.



## What are the Fraud Prevention tools

Any account that is set up with Opayo has the option to use a number of fraud prevention tools as standard.

Each of the tools that are available are in place to ensure you and your shoppers are as protected as possible when it comes to processing transactions.

The tools that are available on your Opayo account are:

- **Address and Postcode verification checks**
- **CV2 (card security code) verification checks**
- **3D Secure for cardholder authentication**
- **Enhanced fraud screening**

All of these tools are available on all accounts with Opayo and at no extra cost.

If you are interested in finding out more about other fraud screening tools we offer give our team a call on **0191 313 0299** and they will be happy to help.

# AVS/CV2

The Address Verification Service (AVS) and Card Verification Value (CV2) check your customer's information to verify the card details used for the transaction. It was introduced by the banking industry to help verify details of CNP transactions (Cardholder Not Present) which enable transactions where the cardholder is not present.

AVS and CV2 checks can be carried out on all ecommerce mail order and telephone order transactions that are placed through your Opayo account.

The aim of these checks is to provide you with additional information on each transaction that will help you reduce the risk of fraudulent transactions.

As standard the AVS/CV2 fraud prevention checks are active on all new Opayo accounts.

## What is AVS/CV2?

### AVS - Address Verification Service

AVS allows you to use the address and postcode numerical values to verify that the card used for the transaction is registered to the address details that have been provided.

When a transaction is processed through Opayo both a Billing address and postcode value is passed through from your website to Opayo. This information is used, and passed through to the card issuing bank to be verified.

The card issuing bank will only check the numerical values that have been provided with the transaction, the bank will not check any of the other characters provided in the address. Opayo will not pass any other characters aside from numbers for the address details in the authorisation request.

AVS checks are available for all UK issued credit and debit cards. The checks are not carried out for overseas transactions.

### CV2 – Card Verification Value

The CV2 check allows you to use the additional 3 or 4 digit security key that is usually found on the signature strip on the reverse of the card.

American Express cards have a 4 digit security key that is located on the front of the card just above the card number.

The CV2 value can be checked on all cards that have been issued within the EU along with the majority of internationally issued cards.

These details are used to verify with the card issuing bank that the 3 or 4 digit security code that is supplied matches the card details that have been entered for the transaction.

# How it works

When a transaction is processed through Opayo we require the basic information for each customer before we can proceed to the card details capture.

**This information includes:**

- Address
- Postcode

**Important - On Opayo's default payment pages the cardholder is able to change the billing address details. If you would like to prevent this go to the settings section within your MySagePay.**

Go to MySagePay > Settings > Settings and click the "edit" button under account settings, choosing "address read only", "no address" or "responsive" in the radial menu will prevent customers from being able to amend their billing address.

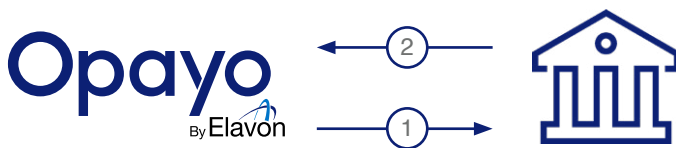
[For more information click here](#)

The customer is then able to enter in their card details – depending on the integration that is being used with Opayo this will either be on your own website, or on one of the Opayo payment pages.

**Here we will capture;**

- Card Number
- Expiry Date
- CV2 Number

This information is submitted to the bank for authorisation. Whilst the authorisation is being carried out, the bank will also validate the address, postcode, and CV2 values.



The bank will then pass the results of the authorisation request back to Opayo along with the results of the address, postcode, and CV2 checks.

Each credit or debit card that is used for a transaction is registered to a billing address.

The banks use the address and postcode details that have been provided to verify that the card being used for the transaction is registered to the address information that has been given.

These results are then passed back to your website and displayed to you in your MySagePay Transaction report.

# Setting your rules

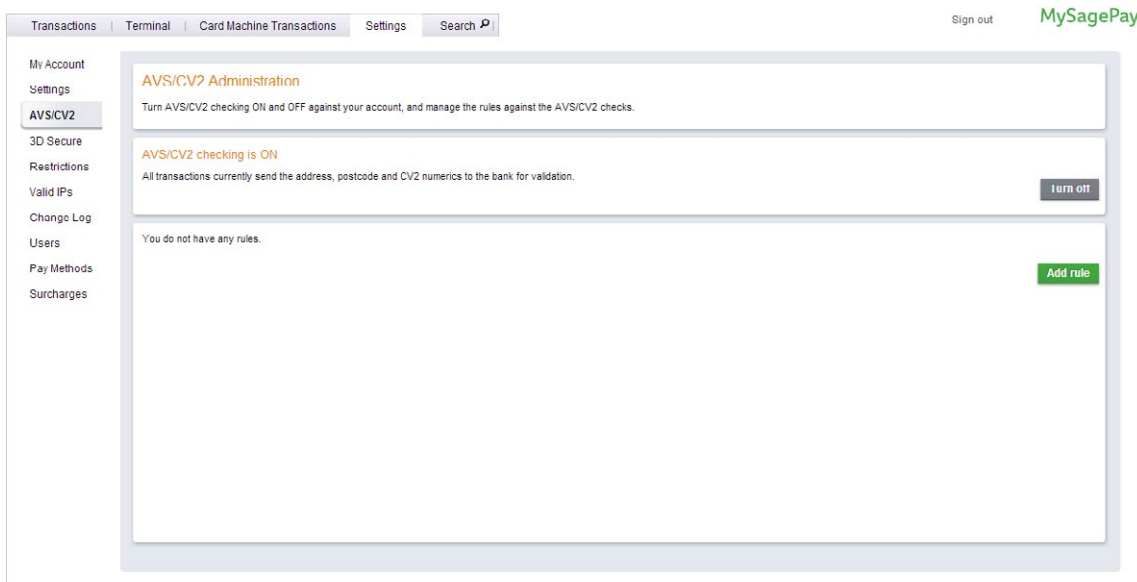
Alongside the AVS/CV2 checks being carried out on your transactions, you are able to apply rules to your account that will either allow, or prevent transactions from processing depending on the results of the checks.

In your MySagePay account you are able to set-up rules to your account that will be applied to all transactions processed.

These rules enable you to define your own restrictions, for multiple price ranges without having to individually review each transaction you have received.

To add a rule to your Opayo account you will first need to login to your MySagePay admin panel as an administrative user, you can do this by going to either the [Test](#) or [Live](#) environments.

MySagePay login page:



**Note: Each rule will need to be added to the Test and Live environments individually. The rules you add to your account DO NOT transfer from Test to Live, or from Live to Test.**

You can find out how to log into our MySagePay account on our [website](#).

After logging into MySagePay select “Settings” followed by “AVS/CV2”. This will open the AVS/CV2 management page within MySagePay.



**Add a new AVS/CV2 rule** ✕

Enter the range for all transactions to which this rule applies.

Start value:  End value:

For transactions within this range:

- Accept DATA NOT CHECKED (bank or card scheme don't check values)
- Accept ADDRESS MATCH ONLY (CV2 check fails, Address check succeeds)
- Accept SECURITY CODE MATCH ONLY (Address fails, CV2 check succeeds)
- Accept NO DATA MATCHES (both CV2 and AVS checks fail)

Here you will be able to add the rules to your account. To add a rule select the “Add Rule” button and you will be presented with a pop-up where you can define the parameters of your rule.

Add a start price and end price and select the restrictions you would like to apply and select.

[For more information on rule bases, and what options are available have a look at our website >](#)



# Understanding your results

Once a transaction has been processed the results of the AVS/CV2 fraud prevention checks are passed back through to your website.

The results are also displayed within MySagePay where you are also able to check these details.

## Result sent back through to your website

When any ecommerce transaction is processed, Opayo will send the results through to your site.

## These results are sent in multiple fields

- AddressResult
- PostcodeResult
- CV2Result

Each of these fields will include a result that can be stored by your site and used to manage your transactions.

## Results in MySagePay

Along with sending the results to your site, the details are also displayed to you within your MySagePay account.

## Each transaction will display the:

- Address Result
- Postcode Result
- CV2 Result

When the results are displayed in MySagePay all 3 will be displayed individually.

These fields will be displayed in your MySagePay as columns in the transaction list titled

– CV2, Add (Address), PC (Postcode).

# Common Questions

## Does AVS/CV2 impact the authorisation process?

The AVS/CV2 fraud prevention checks do not have any impact on the authorisation process.

Once authorisation has been granted on a transaction the funds will be shadowed from the account in preparation to be transferred into your bank account.

If the transaction is then rejected based on the rules you have in place then the authorisation will still be in place, and so will the shadow.

[To find out more about shadows you can check our website >](#)

## I have AVS/CV2 turned on in MySagePay but the checks are not being carried out?

If you have AVS/CV2 turned on in your MySagePay account but the checks are not being carried out, you will need to check the details of the transaction registration post that is made to Opayo.

When any ecommerce transaction is processed through Opayo, your website will send us a post with all of the transactional information.

Included in this post is a field ApplyAVS/CV2= which contains a numerical value. Each value refers to a specific rule that will overwrite anything you have set in your MySagePay account.

Those values are:

**0 = If AVS/CV2 enabled then check them. If rules apply, use rules. (default)**

**1 = Force AVS/CV2 checks even if not enabled for the account. If rules apply, use rules.**

**2 = Force NO AVS/CV2 checks even if enabled on account.**

**3 = Force AVS/CV2 checks even if not enabled for the account but DON'T apply any rules.**

If you would like your website to only carry out CV2 checks based on the rules you have in your MySagePay admin panel, you must ensure that the **ApplyAVS/CV2=0**.

## Who checks the AVS/CV2?

Opayo do not carry out the actual AVS/CV2 fraud prevention checks. This information is captured from your shopper by Opayo but is passed through to the banks at the authorisation stage for the details to be checked.

## Can I have more than one AVS/CV2 fraud prevention rule on my account?

Yes you can. There are no restrictions to the amount of rules that you can have on your account at any one time.

### **Is there a cost for using AVS/CV2?**

The AVS/CV2 fraud prevention tool is a free addition to your Opayo account that does not cost you to use.

### **How long does it take for the results to come back?**

As soon as the transaction has been sent to the bank for authorisation the AVS/CV2 checks will be carried out by the banks.

Once the authorisation response has been received by Opayo we will display the AVS/CV2 results to you within your MySagePay admin panel, and return the results to your website in the transaction response post.

### **Why do I get no results for certain transactions?**

Unfortunately Opayo are not able to obtain Address and Postcode results for all international transactions that are processed through our systems.

As Opayo are a UK Payment Gateway we cannot always obtain and return results for transactions that are processed using cards, addresses, and postcodes that are outside of the UK.

### **Addresses from the Republic of Ireland do not have postcodes, how do I process transactions?**

All addresses from the Republic of Ireland are not issued with postcodes, because of this Opayo are unable to check the details with the bank and apply the address and postcode checks to a transaction from this country.

When processing a transaction through your Opayo account with an address from the Republic of Ireland you are NOT required to enter a postcode in order for the transaction to be processed.

The Opayo system is aware that postcodes are not issued in the Republic of Ireland. However, we advise entering "000" into the field for ecommerce transactions to be processed as some merchant acquirers still require this information.



# Benefits

There are a number of benefits to using the AVS/CV2 fraud prevention tools on your Opayo account.

- ✓ Real time fraud analysis.
- ✓ Address, Postcode, and Security Key verification.
- ✓ Add rules and restrictions to your account limiting the risk of fraud.
- ✓ Free of charge – there is no cost to use the AVS/CV2 fraud prevention tools.

When using the AVS/CV2 fraud prevention checks you give your business a better chance of preventing fraudulent transactions being processed through your account. You can use the checks that are available to manage your own transactions, and ensure that transactions are processed only when they have met the criteria that you have set for your business



# 3D Secure and PSD2

3D Secure is otherwise known as Verified by Visa, Mastercard Secure Code, or American Express Safekey and is an additional fraud prevention tool that is available on your Opayo account. 3D Secure requires a shopper to have registered their card as part of the scheme to add another layer of protection to your account when transactions are processed.

## Strong Customer Authentication

The Revised Payment Services Directive (PSD2) was introduced as a follow-up to the original Payment Services Directive by the European Commission, it took effect in January 2018. The aim is to bring in new laws to increase customer protection, foster innovation, and inspire pan-European competition.

A key element of PSD2 is the introduction of the Regulatory Technical Standards on Strong Customer Authentication (SCA), it has been introduced to help combat fraud by improving customer security whilst reducing the liability held against businesses for unauthorised transactions. It makes payments more secure for both your business and your customer by adding an extra layer of protection known as two-factor authentication (2FA).

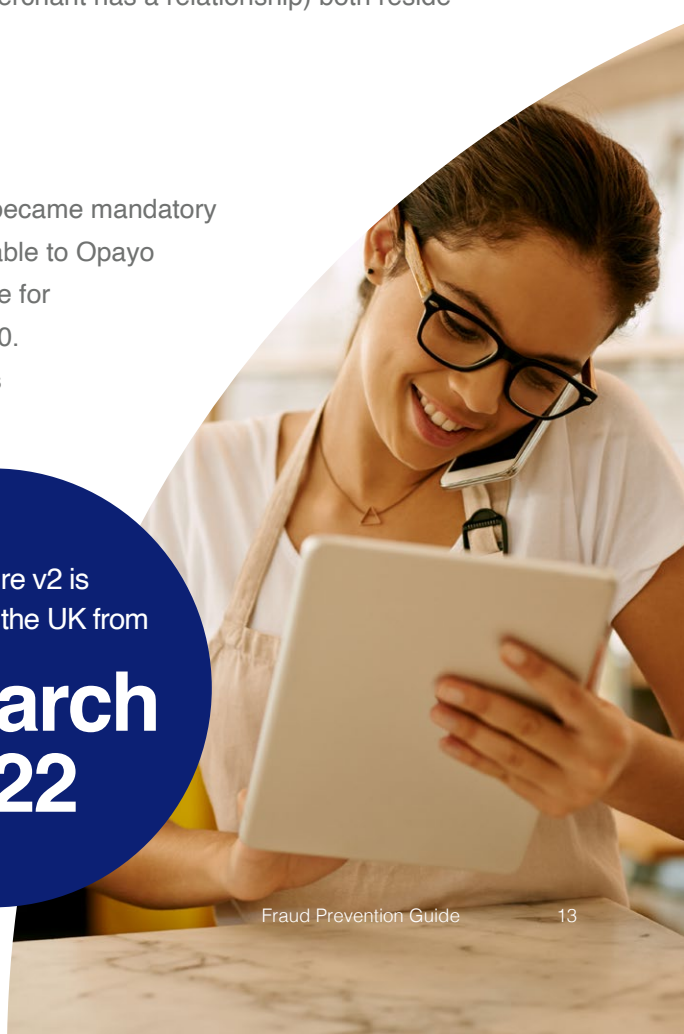
SCA applies to card-based ecommerce transactions (including digital wallets backed by cards), where both the card issuer (i.e. financial institution with whom the cardholder has a relationship) and the acquirer (i.e. financial institution with whom the merchant has a relationship) both reside within the European Economic Area (EEA).

### Implementation Period

The current 3D Secure implementation was supported until the end of 2020, at which time 3D Secure version 2 became mandatory worldwide. 3D Secure version 2 functionality is now available to Opayo customers on our test and live environments. The deadline for ecommerce compliance in Europe was 31 December 2020. In the UK, the new deadline for ecommerce compliance is 14 March 2022.

3D Secure v2 is  
mandatory in the UK from

**14 March  
2022**





## How will the shopper be authenticated?

All ecommerce transactions where the cardholder is in-session, must perform 3D Secure authentication. During 3D Secure authentication, a challenge authentication can take place, or a frictionless authentication can also take place.



### Something you know

- Password
- Passphrase
- PIN
- Sequence
- Secret fact



### Something you own

- Mobile phone
- Wearable device
- Smart card
- Token



### Something you are

- Retina scan
- Fingerprint
- Voice pattern
- Facial recognition

## Exemptions to SCA

There are several exemptions to SCA that may be requested to improve the payment experience. You first need to speak with your acquirer to get their approval of any exemptions you choose to use. Once your acquirer has advised of suitable exemptions for your business model, you can request an exemption on a per transaction basis when submitting your transaction request to Opayo. If you choose to use an exemption, any chargeback liability is passed to you for the transaction. The card issuer may not always agree with your exemption. In this instance, they may return a 'soft decline' and request that 2FA is performed.

[For more information on SCA please take a look at our guide here >](#)

# What is 3D Secure

3D Secure is an online version of password protection that is only available on ecommerce transactions.

When a shopper processes a transaction through an account with 3D Secure active, they are required to enter their password or OTP (one-time-password) verification in order for the details to be validated against the card they are using for the transaction.

**There are 3 card issuers that currently support 3D Secure when transactions are being processed.**



## Verified by Visa

Supports all Visa cards as part of the 3D Secure scheme such as, Visa Credit, Debit, Delta, Electron.



## Mastercard Secure Code

Supports all Mastercard issued cards such as, Mastercard Credit, Debit, UK Maestro, and International Maestro cards.



## American Express SafeKey

Supports American Express issued cards through the scheme.

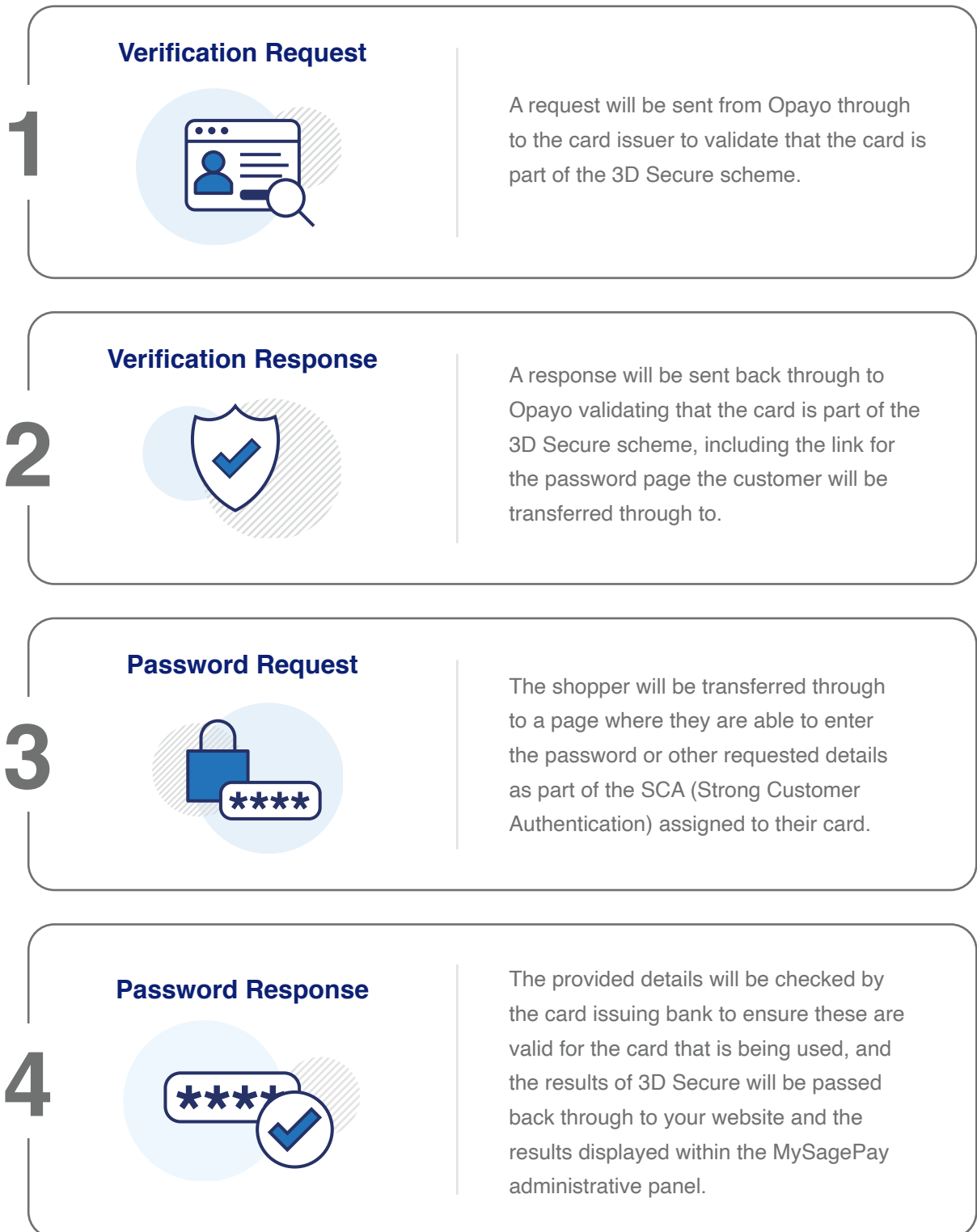
If a shopper has any of the above issued cards they will be able to register their card with 3D Secure, assign a password and a mobile number to be used when they process a transaction.



# How it works

When an ecommerce transaction is processed through a website using Opayo, 3D Secure is available to use on the payment.

3D Secure is a 4 step process that checks if the card is registered with the scheme and prompts the customer to enter a password in order for the transaction to be verified.





Once a customer has selected the items they want to purchase, a transaction registration is sent from your website through to Opayo for the payment process to begin.

After this has been received by Opayo and 3D Secure is active, a request will be sent through to the card issuer – VISA, Mastercard, or American Express to validate that the card is registered as part of the 3D Secure scheme.

Confirmation that the card is part of the scheme will be returned back through to Opayo along with the ACSURL. The ACSURL is a link to a page of the card issuing bank that the shopper will be transferred through to so that they can enter the password that is assigned to the card.

The customer will enter the password which will then be validated and the results returned through to Opayo. Opayo will then return the results of 3D Secure to the website and present them in the MySagePay Admin Panel.

3D Secure integration is controlled and hosted by Opayo whether you are using either the Form or Server method of integration.

For Direct and Pi (REST API) integration, 3D Secure will be hosted on your website however the process will remain the same. You will need to manage the integration for 3D Secure with Direct and Pi yourself. Details of this integration can be found in the Direct or Pi protocol guide on our website.

[To find out more about PSD2 and 3D Secure you can check our website >](#)



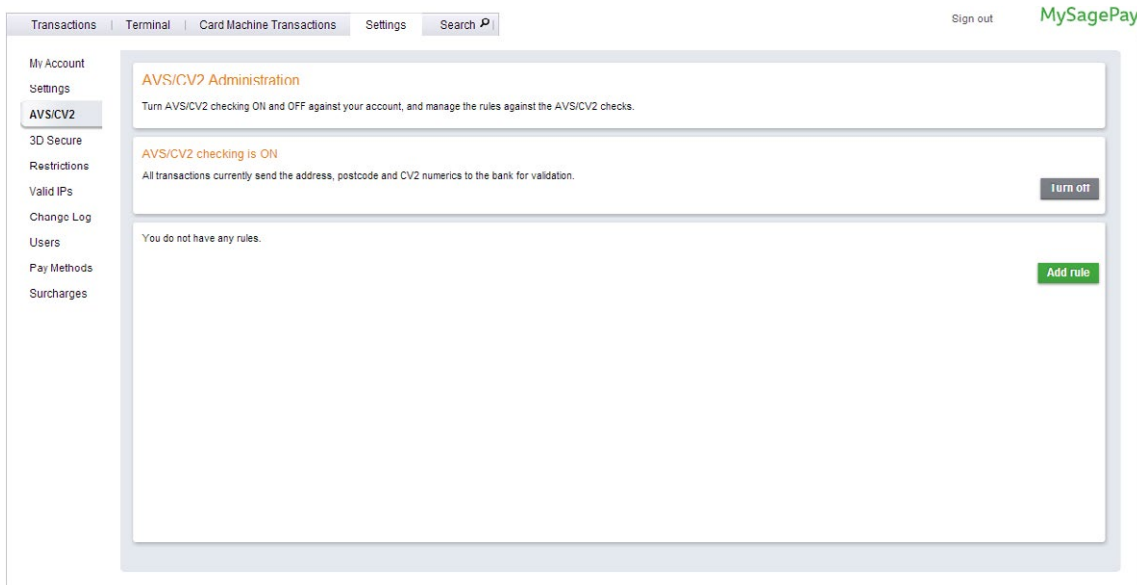
# Setting your rules

3D Secure also offers you the ability to add rules to your Opayo account that will accept or reject transactions based on the results of the 3D Secure checks.

The rules that are added to the account allow you to define your own restrictions across multiple price ranges without having to individually review each transaction. To add rules to your account you will first need to login to either [Test](#) or [Live](#) MySagePay as an administrative user.

All rules that have been added to the account will be applied to all transactions that are processed.

Once logged into MySagePay select “Settings” followed by 3D Secure. This will open the 3D Secure management page within MySagePay.



**Note: Each rule will need to be added to Test and Live individually. Any rules added to the account DO NOT transfer from Test to Live, or from Live to Test.**

[More information on logging into MySagePay can be found on our website >](#)





**Add a new 3D secure rule** ✕

Start Value: \*  End Value: \*

For transactions within this range:

- Perform the 3D secure authentication
- Accept non-3D secure cards to be authorised
- Accept authorisations when MPI errors occur
- Accept cards from non-3D secure issuers to be authorised
- Accept 3D secure failures to continue for authorisation

Once on the 3D Secure management page you are able to add rules to your account. To add a rule select the “Add Rule” button and you will be presented with a pop-up where you can define the parameters of your rule.

Add a start price and end price and select the restrictions to apply.









[More information on rules bases can be found on our website >](#)

# Understanding your results

Once a transaction has been processed the results of the 3D Secure fraud prevention checks are passed back through to your website.

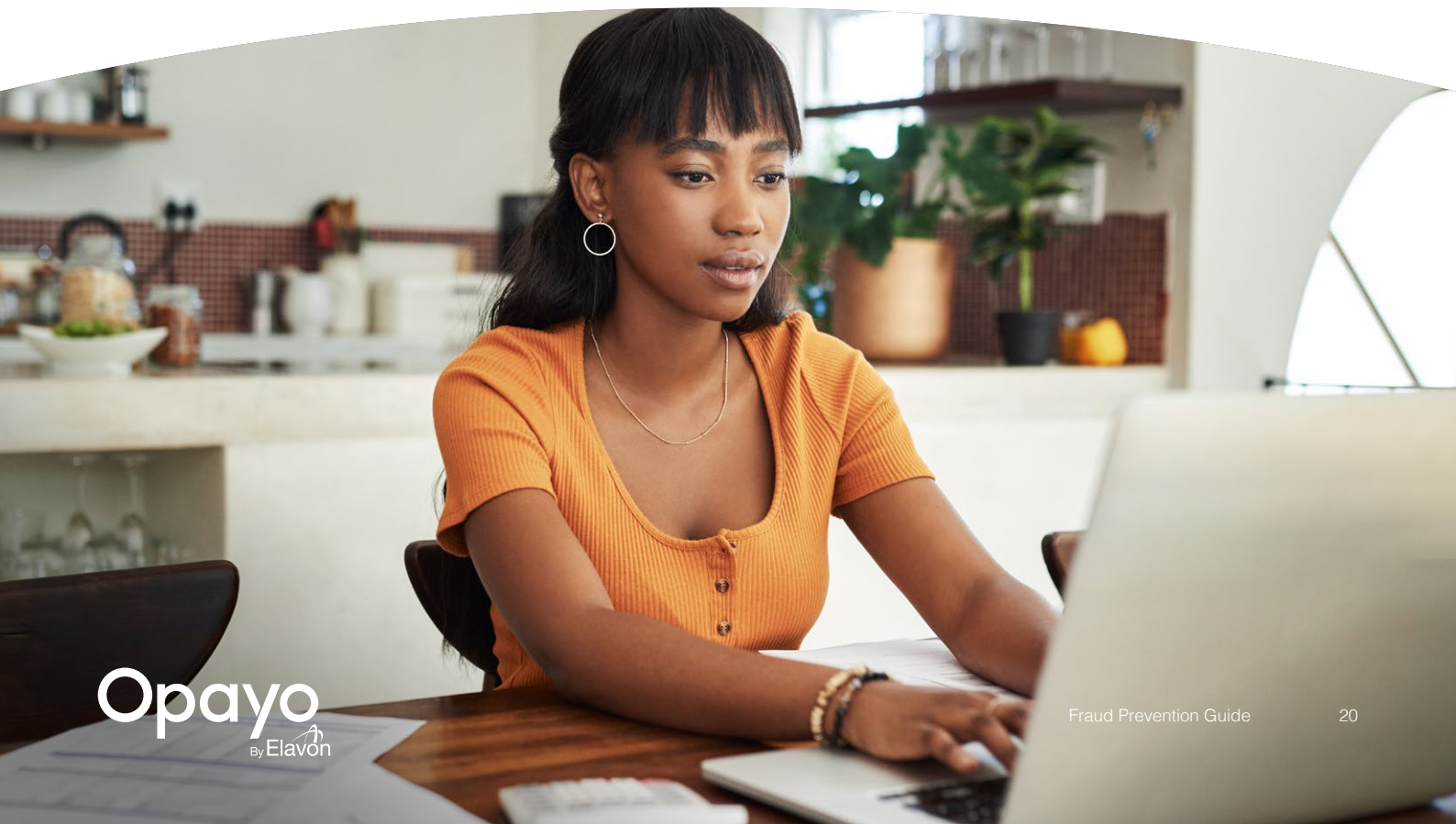
Each transaction that is processed with the 3D Secure fraud prevention checks will have individual results which are displayed in MySagePay.

There are a number of possible 3D Secure results that will be sent back through to your site and displayed within MySagePay.

3D Secure Status	MSP Display	Description
OK		3D Secure has been passed successfully
Attempt Only		3D Secure has not completed fully - check with bank for liability shift confirmation
Incomplete		3D Secure was unable to complete
Not Available		3D Secure validation could not be carried out for the tx
Not Checked		No 3D Secure checks were carried out on the tx
Not Authed		The cardholder failed to pass 3D Secure verification
Can't Auth		The card issuer is not part of the 3D Secure scheme
Error/Invalid/Malformed		Problem processing 3D Secure - uncommon status

All of the above information will be returned directly to your website in a post along with the status of the transaction.

The results will also be displayed in your MySagePay administrative panel as a shield in the 3-D column.



# Common Questions

## Does 3D Secure impact the authorisation process?

When a transaction is processed using the Opayo gateway it is sent for 3D Secure before it is sent for authorisation.

If a transaction is rejected based on the 3D Secure rules that are in place, then the transaction will not be sent for authorisation.

## How is 3D Secure added to an account?

When an account is set up with Opayo and the merchant account information has been received, a request will be sent from Opayo to the bank for 3D Secure to be set up.

This can take up to 15 working days to be confirmed by the bank.

If you are a Barclays merchant services customer, you will need to contact the bank directly for 3D Secure to be set-up. The details will then need to be passed directly to Opayo.

If you are an American Express customer, your merchant number is automatically enrolled to SafeKey by Opayo.

## Is there a charge for 3D Secure?

Although 3D Secure is an additional fraud prevention tool that is available through the Opayo systems, there is no charge to use this service.

## How long does it take for 3D Secure results to be returned?

Because 3D Secure validation is carried out before the transaction is sent for authorisation the results for the checks will be returned back through to your website along with the status of the transaction.

## Is 3D Secure available to all transactions processed through my account?

Unfortunately not, 3D Secure as a scheme is only available to ecommerce transactions that are processed through your account.

Alongside this, 3D Secure is only available on VISA, Mastercard, and American Express transactions and no other cards.

As 3D Secure is a scheme that is controlled by the card issuers themselves, it is limited to the cards that are controlled by each.

## 3D Secure is turned on in my account but no results are being received

If you have 3D Secure turned on in your MySagePay account but the checks are not being carried out you will need to check the details of the transaction registration post that is made to Opayo.

When any ecommerce transaction is processed through Opayo your website will send us a post with all of the transactional information.

Included in this post is a field Apply3-DSecure= which contains a numerical value. Each value refers to a specific rule that will overwrite anything you have set in your MySagePay.

### Those values are

**0 = If 3D Secure checks are possible and rules allow, perform the checks. (default)**

**1 = Force 3D Secure checks even if not enabled on the account and apply any rules.**

**2 = Force NO 3D Secure checks even if enabled on account. Following the SCA mandate, we recommend you do not use this flag. If the cardholder fails authentication, and the request is sent for authorisation, expect the payment to be declined by the card issuer.**

**This field is ignored for PayPal transactions.**

**3 = Force AVS/CV2 checks even if not enabled for the account, DON'T apply rules.**

If you are using protocol 4.00, and option Apply3-DSecure=2 is used, a valid ThreeDExemptionIndicator must be provided. See our development documentation for more information.

For transactions taken under protocol 4.00, we do not recommend using this flag.

## Can I have more than one 3D Secure rule on my account?

Yes, there are no restrictions to the volume of rules that you can have on your Opayo account at any one time.

As long as the price ranges that are set for the rules do NOT overlap you are able to have as many, or as few rules as you would like.

## Are all transactions that pass 3D Secure covered by the liability shift?

When a transaction successfully passes 3D Secure there is a chance that the transaction will be covered by the liability shift.

Opayo cannot guarantee that all transactions processed through 3D Secure will be covered and we would advise that any transactions you would like confirmation of the liability shift is raised with your merchant bank.

As the card issuing bank is the party that is covering the liability for the transaction, it will be the bank who will state what will be covered and what will not.



# Benefits of Opayo's Upgrade to 3D Secure Version 2

During a 3D Secure authentication, how the authentication is performed is up to the card issuer. It's possible to achieve SCA with 3D Secure version 1, however 3D Secure version 2 makes this much easier.

When 3D Secure version 2 is enabled, it is estimated that only 5% to 10% of authentications will result in the cardholder having to be re-directed to their bank's 3D Secure page to enter 2FA. Most authentication requests will result in a frictionless authentication with an authorisation rate of up to 90%. What's more, liability for unauthorised transactions passes to the card issuer, saving you time and money on potential disputes.

- ✓ Added security and protection for your business and your customers
- ✓ Increased cardholder confidence when transacting with your business
- ✓ Reduced fraud and chargebacks - liability shifts to the card issuer
- ✓ Frictionless authentication where the customer doesn't even realise that authentication has taken place e.g. biometric authentication using fingerprint, facial or voice recognition
- ✓ Improved risk-based decisions using rich cardholder data leading to higher approval rates
- ✓ Full support for all available exemption types and payment device types

By using the 3D Secure fraud prevention tool on your account you are adding another layer of protection to your business when combatting online fraud.

3D Secure can be used to help manage, and validate your transactions remotely without the need for every transaction to be manually checked.



Authorisation rates  
of up to  
**90%**

# Additional Restrictions

The restrictions section is where you can manage IP addresses, countries, and cards you would like to prevent from processing transactions through your account.

There are four options to choose from when deciding what you would like to block.

## Blocking IP addresses

Here you can block specific or ranges of IP addresses from processing transactions through your account.

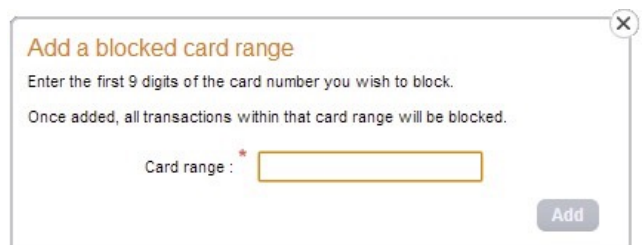
[Find out more about blocking IP addresses.](#)



## Blocking card ranges

By entering the first 9 digits of a specific card you will prevent any card beginning with those numbers from processing a transaction through your account.

[Find out more about blocking card ranges.](#)

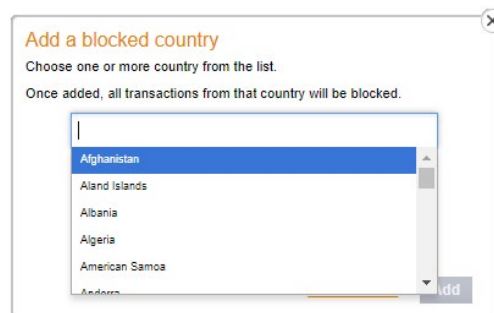


## Blocking countries

Blocking a country will stop any transactions from being accepted when the IP address used is from a country you have.

To block a country you will need to select it from a list provided by Opayo.

[Find out more about blocking countries.](#)



## Blocking issuing countries

By selecting to block a country you will prevent any cards that are issued in that country from being able to make a purchase through your account.

To block an issuing country, you will need to select it from a list provided by Opayo.

[Find out more about blocking issuing countries.](#)







# Enhanced Fraud Screening

Our in house enhanced fraud screening system is an extensive risk management platform that performs reviews on transactions that have been processed through your Opayo account.

## What is enhanced Fraud Screening?

Opayo's enhanced fraud screening monitors all your customer data in real time, spotting anomalies to enable you to outsmart risk, protect your customers and increase revenue. All the results are then passed back through to Opayo to be displayed within your account.

All results provided by the Opayo enhanced fraud screening tool are advisory only to give you an indication of how likely it is that the transaction is legitimate or fraudulent. With that information you can then choose to let the transaction proceed as normal or to intervene and void (before midnight) or refund.

# How it works

When a transaction is processed through the Opayo system, the details of that individual payment are passed through to Opayo's fraud screening service for analysis to be carried out. Using adaptive behavioural analytics to spot and block fraud our solution continually improves and adapts to new risks.

Opayo's fraud screening tool will take all of the information that has been captured and use this information to build a risk score that will be available to you in real time.

Once the transaction information has been passed to Opayo's fraud screening systems for analysis against a fraud and risk ruleset, a Risk score will be produced calculating the likelihood of the transaction being legitimate or fraudulent.

All transactions begin with a score of 0 when the transaction is first submitted to fraud screening for analysis. Each rule that is triggered increases the percentage risk of the transaction. Should the risk level exceed an acceptable threshold an advisory alert appears in MySagePay (MSP).

Once the risk score has been assigned, the score will then be available in the MSP portal and via our API . We provide the score as well as a summary of the rules the transaction triggered.





## What data is checked?

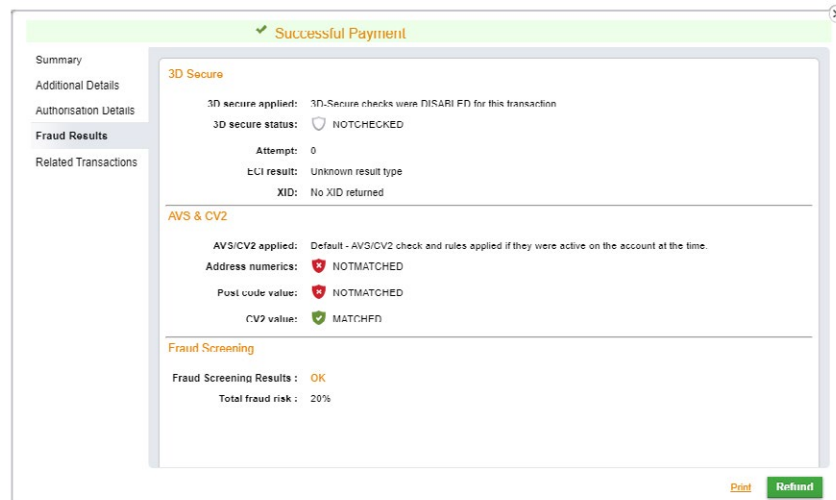
Each time a transaction is processed Opayo's fraud screening tool checks a number of variables including customer details such as their name and email, billing and delivery addresses, as well as analysing data and patterns related to transactions and customer behaviour. The tool also compares transaction histories across similar businesses, within the same merchant category code, and similar shoppers.

# Understanding your results

After a transaction has been processed, and scored, the results will be displayed within MySagePay.

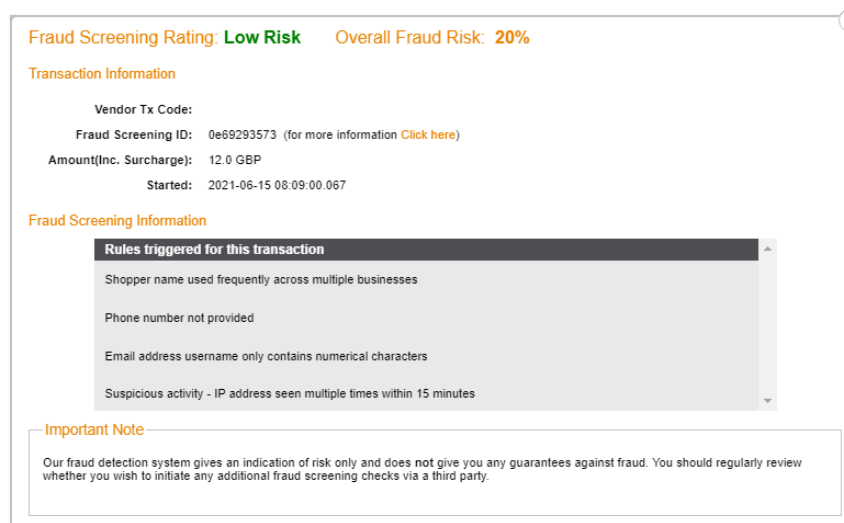
The results from the fraud analysis will be available in the Risk level and Score range. The risk score of the transaction can be seen if you hover over the shield displayed in MySagePay.

To view the breakdown of the results for the fraud screening, click on the transaction and then the Fraud Results tab.



Here, select the Fraud Screening Result displayed as either OK or REJECT. This will open a separate window with the summary of the fraud results including the triggered rules.

The total fraud score will give the numerical % score that has been assigned to the transaction. To view a summary of rules triggered click the Fraud Screening Result.



**Important: All of Opayo's fraud screening results, and scores, are advisory ONLY and are simply a recommendation to help you decide how to proceed.**

Below is an overview of the current rule set that a transaction can trigger in MySagePay. Please note a rule will only trigger if suspicious activity is suspected, if a specific rule wasn't triggered then that particular activity wasn't deemed suspicious at that time.

Each transaction will be assigned a fraud score based on the rules that have been triggered.

#### Merchant rules displayed in MSP\*

Suspicious activity - large number of transaction attempts using cards from this issuer

Suspicious activity - card used in multiple countries recently

Suspicious shopper activity - card used elsewhere at exactly the same time

Suspicious shopper activity - >15 transactions in <1 second

Suspicious activity - IP address seen multiple times within 15 minutes

Unusual account activity - transaction exceeds your processing profile yesterday

Unusual account activity - transaction exceeds your typical weekly profile

Unusual account activity - transaction exceeds your typical monthly profile

Unusual account activity - you're seeing a large number of declines from your acquirer

Unusual spend activity - numerous payments of similar value already declined

Unusual spend activity - low value payment

Unusual spend activity - numerous payments of similar value already declined across multiple businesses

Unusual shopper activity - numerous high value payments within 24h

Unusual shopper activity - CV2 missing or during a previous transaction the shopper failed a CV2 check

Unusual shopper activity - during a previous transaction the shopper failed/partially matched on the postcode AVS check

Unusual shopper activity - during a previous transaction the shopper failed/partially matched on the house number AVS check

Transaction value three times higher than your 90d rolling average

Transaction value five times higher than the 90d rolling average for similar businesses

The transaction value is lower than your average

Transaction time during unsociable hours

Transaction time unusual for your business

Shopper name used frequently on your account

Shopper name used frequently across multiple businesses

## Shopper rules displayed in MSP\*

Suspicious activity - card declined recently

High volume of transactions seen against this shopper's card

High value of transactions seen against this shopper's card

Unusual shopper activity - multiple phone numbers seen with this card

Unusual shopper activity - multiple email addresses seen with this card

Unusual shopper activity - multiple billing or shipping addresses seen with this card

Unusual shopper activity - multiple IP addresses seen with this card

Unusual spend for this card

The payment card was issued abroad

Shopper card issued in a country you see infrequently

Billing and delivery addresses are different

Shipping address is in a different country to the billing address

PayPal has reported an address mismatch

New billing or shipping address used by a returning shopper

The billing or shipping address has been previously associated with fraudulent activity

Non-residential/business address used

New IP address used by a returning shopper

New mobile number used by a returning shopper

The phone number provided has been previously associated with fraudulent activity

Phone number not provided

New email address used by a returning shopper

The shopper's email address doesn't contain any part of the cardholder name

Email address username only contains numerical characters

Email address has been previously associated with fraudulent activity

Email address has been previously associated with suspicious activity

\*Rules will be reviewed regularly and may be subject to change

## What to check

When reviewing the results of the Opayo's fraud screening verification it is important to note:

- **Low risk** – when a transaction is marked as low risk it is an indication that the transaction doesn't appear to be fraudulent. A transaction that is low risk is usually acceptable to process without the need for further investigation.
- **High Risk** – when a high risk score has been returned, we advise that further investigation is carried out on the transaction, such as contacting the customer for proof of address, and reviewing the transactional breakdown. High risk transactions indicate a substantial risk to your business and as a rule should be processed with caution.

When the score has been provided the breakdown will provide a summary of the rules the transaction has triggered so you can see exactly what data elements were unusual or suspicious and contributed to a higher risk score calculation.



# Common Questions

## **A low risk transaction was advised as 'ok' but has since received a chargeback. Who is responsible for this?**

All risk levels that are provided by Opayo's fraud screening tool are advisory only, and should be used with the other fraud prevention tools that are available with all Opayo accounts.

When speaking with the Opayo team, the recommendation provided is also strictly advisory and a final decision on processing the transaction is down to you (the vendor).

If a transaction has been identified as Low Risk it simply indicates that at the time of processing there was no evidence to suggest possible fraudulent activity. By using the additional fraud prevention tools that are available in your account alongside Opayo's fraud screening tool, the risk of fraud chargebacks can be limited.

Any chargebacks based on decisions using the Opayo's fraud screening tool scores only is the responsibility of the vendor.

## **Is there a cost for using Opayo's fraud screening tool system?**

No, Opayo's fraud screening service is provided to each Opayo customer as standard.

## **How long does it take for Opayo's fraud screening tool results to be returned?**

Usually Opayo's fraud screening results are returned instantly to and displayed within MySagePay on the transactional details screen.

## **I have a transaction that does not have an Opayo score, what do I do?**

If you have a transaction that has not yet been issued with an Opayo fraud screening score you will first need to wait 24 hours for the transaction to be updated.

After 24 hours have passed, if the transaction still has not yet been updated with a score email support@opayo.io including vendor name, vendor tx code, and date and time of the transaction.

The Opayo team will then arrange for the transaction to be re-submitted to Opayo's fraud screening tool for a score to be returned.

## **Do I have to turn Opayo's fraud screening tool on in my Opayo account?**

No, Opayo's fraud screening tool is active as standard on all Opayo accounts and does not need to be activated in order to get results for your transactions. NB: The additional fraud tools, including AVS, CVV and 3-D checks, will need to be enabled by you – we advise you configure and activate these settings before you go live and review those settings regularly.



## Can I add my own rules to Opayo's fraud screening tool?

No, the Opayo fraud screening ruleset is centralised and managed by Opayo. The product team periodically review the ruleset and scoring configuration for optimal efficiency.

## Can I automatically accept or reject transactions based on Opayo's fraud screening score?

No, Opayo's fraud prevention system is an advisory service only and cannot automatically reject transactions based on the results.

The Opayo fraud screening tool or resulting score will not alter a transaction status, vendors must intervene to void or decline transactions if they wish to further investigate the legitimacy of a purchase.

## I'm not getting any fraud screening results for my test transactions, is this normal?

Completely, although you can test all of the other fraud prevention tools, the Opayo fraud screening service is only available for live transactions and does not return any results on the test platform.

## Do international card-based transactions and PayPal transactions get scored by Opayo?

Yes, these transactions can be scored by Opayo's fraud screening tool.

## Are there any transactions that will not get an Opayo fraud screening result?

The only transaction types that will not return an Opayo fraud screening score is a refund.

All other transaction types will return an Opayo's fraud screening score:

- **Payment** – Opayo fraud screening score returned with order being processed.
- **Deferred/Release** – Opayo fraud screening score issued at the deferred stage of order.
- **Authenticate/Authorise** – Opayo fraud screening score issued at both stages of the order.
- **Repeat** – Opayo fraud screening returned with order being processed.

NB: all credit and debit card and PayPal transactions will be scored, please note that at present transactions processed using the international payment methods Sofort, iDEAL, giropay and EPS will not return a fraud screening result.



# Benefits

There are a number of benefits for your business when using Opayo's fraud screening on your transactions.

- ✓ Transactional analysis.
- ✓ Risk assessment on all transactions processed.
- ✓ Additional layers of protection – Opayo fraud screening is another fraud prevention tool offered.
- ✓ Free of charge – there is no cost to use Opayo's fraud screening tool.

Opayo fraud screening enables you to review transactions that have been processed through your account, along with providing detailed analysis of the information that has been submitted with each transaction.

The risk levels offered by Opayo's fraud screening tool that is assigned to each transaction improves account management and gives an overview of the fraudulent risk posed every time a payment is received through your Opayo account.





# ACI Fraud Management

ACI Fraud Management is a fraud prevention tool that is available to all Opayo customers at an additional cost.

Running in place of Opayo's fraud analysis tool ACI Fraud Management provides real time transactional analysis that can be used to effectively and automatically manage transactions that have been processed through any Opayo account.

## What is ACI Fraud Management?

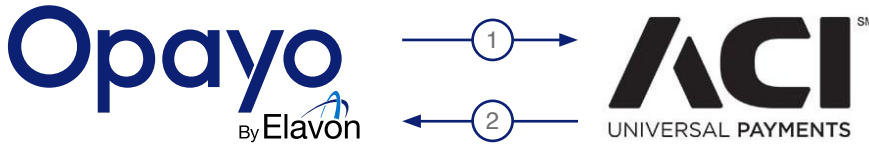
ACI Fraud Management is a leading independent fraud prevention company working with payment gateways to limit and fight payment fraud.

Using real time fraud analysis to prevent fraudulent activity on Opayo accounts and increase revenue by reducing loss.

ACI Fraud Management solutions are tailored to the specific needs, and market of the customer to offer in depth protection against fraudulent activity.

# How it works

When ACI fraud screening is active on an account the transactional information is passed through to the ACI Fraud Management platform.



Abbreviation	Element
Accept	The transaction has been approved by ACI and will be sent for authorisation.
Challenge	The transaction has triggered rules in the ACI fraud screening platform and requires further investigations.
Deny	The transaction has not passed the fraud screening checks and has been rejected. The transaction will not be sent for authorisation.
Not Checked	The transaction was unable to be checked by the ACI platform and no results were returned.

The response that has been provided from the ACI Fraud Management platform will then be passed back through to the website in the form of a field called FraudResponse. This field will include one of the four possible responses that will then be logged by the websites systems.

Each business who uses ACI fraud screening will have access to their own administrative (ACI CSI Portal) platform directly from ACI where they can review and manage transactions that have been processed through the account.

As the results are not displayed within MySagePay any transaction reviews on the fraud screening MUST be performed directly within the ACI CSI Portal.

Once the transaction has been reviewed by the ACI Fraud Management platform, they will then run the details against the rules that have been put in place on the account.

# Setting your rules

Choosing ACI Fraud Management will require you choosing which rule set you wish to be set up in order for the fraud screening to be undertaken.

During the onboarding process, you will be presented with a pre-defined list of rules that are available to the specific business sector they relate to. You can then choose the most appropriate to your business.

Each rule that is available will be assigned either – accept, challenge, or deny and will apply to checks.

The available rules will then be applied to the account and all transactions that are subsequently processed will be screened by these sector specific rules.

# Understanding the results

When a transaction has been processed through the ACI fraud screening tool a response with either accept, challenge, or deny will be sent from Opayo directly to the website.

This status will determine if the transaction has been sent onto the bank for authorisation, or denied if not.

The results are not displayed within MySagePay and all information on each transaction that has been processed through ACI Fraud Management will be available to review in the ACI platform directly.

The ACI Fraud Management platform will identify what rules the transaction has triggered and how the status has been assigned.



## Common Questions

### Is there a cost for using ACI Fraud Management?

Yes, as the ACI fraud screening tool is an additional feature added to the account there is a charge for using this.

[To find out more about ACI fraud screening and to add this to your account contact our Sales Team on 0800 084 1821.](#)

### Why do the ACI results not display in MySagePay?

Due to the integration of the ACI platform with the Opayo gateway there is currently no way to display the transaction state from ACI in MySagePay.

All of the information surrounding the transaction is available within the ACI CSI portal and can be viewed directly there.

### How do I get the ACI transaction ID?

In order to get the ACI transaction ID you will need to perform a getFraudScreenDetail request from the Opayo Reporting and Admin API.

Once this request has been performed a response will be sent back through to you from the Opayo platform including the status of the transaction (accept, challenge, deny) along with the ACI ID that can be used to locate the transaction within the ACI Fraud Management portal.

### How does a Deny response get displayed in MySagePay?

If you have ACI active on your account and a transaction has been denied by ACI it will be shown as a Failed transaction within MySagePay, with the message –

[Transaction Rejected by the Vendors rule base.](#)

Due to the transaction not passing the ACI fraud screening it has failed the fraud prevention rules you have in place and will not be processed through the account.

### If I get ACI fraud screening on my account will training be provided?

Yes, once you have signed up for ACI Fraud Management training will be provided by the Opayo team on using the CSI portal and managing your transactions.

### **How long do the results take?**

ACI Fraud Management is real time fraud prevention and as such the results are returned almost instantly.

### **Will I still be able to use the other fraud prevention tools alongside ACI?**

When ACI Fraud Management is active on your account you will be able to use the AVS, CV2, and 3D Secure fraud screening alongside the additional layer provided by ACI.

The only fraud prevention tool that is no longer available will be Opayo's fraud screening tool which will be replaced on your account.

Instead of Opayo's fraud screening results a red ACI transaction status result of either Accept, Challenge, or Deny will be returned.

### **What happens if I don't get any results from ACI Fraud Management for my transactions?**

If ACI Fraud Management is unable to provide a result for a transaction or the platform is unavailable the Opayo system will submit the transaction to Opayo's fraud screening tool in order to obtain a rating for the transaction.

Opayo's fraud screening tool will then provide a risk level and rating for the transaction as normal.





## Benefits

ACI fraud screening provides a number of benefits when being applied to any business.

- ✓ Real time fraud analysis.
- ✓ Business sector rule bases.
- ✓ Account performance and reviews.
- ✓ Review transactions reactively.
- ✓ Additional layer of protection.

All of the features available with ACI Fraud Management will improve the protection offered to businesses alongside the current, standard fraud prevention tools.

ACI fraud screening is a premium service offered to Opayo customers that can be applied to their accounts.





**We understand that your business never sleeps, that's why our UK based support team are here to help you 24/7:**

Call us

Write to us

Or visit

**Email**

Quorum Business Park  
Benton Lane  
Newcastle upon Tyne  
NE12 8BX  
United Kingdom

[www.opayo.co.uk](http://www.opayo.co.uk)



ELAVON FINANCIAL SERVICES DAC (UK Branch), trading as Opayo.  
Registered in England and Wales – Establishment No. BR022122.  
Registered Office at Level 15 City point One Ropemaker Street, London, EC2Y 9AW.