ULTRADATA®

A Guide to Rule Implementation for Fraud Interceptor

User Manual

Edition 1.9

The Ultradata office addresses are:

Melbourne (Head Office)
Ultradata Australia Pty. Ltd.
1919 Malvern Road
Malvern East VIC 3145 Australia

Phone: +61 3 9291 1600
Fax: +61 3 9885 2222

Sydney Office
Ultradata Australia Pty. Ltd.
Level 19, 6 O'Connell Street
Sydney NSW 2000 Australia

Phone: +61 2 8264 2100
Fax: +61 2 8264 2111

Perth Office
Ultradata Australia Pty. Ltd.
6 Centro Avenue
Subiaco WA 6008 Australia

Phone: +61 8 9489 7100
Fax: +61 8 6380 1342

New Zealand
Ultradata New Zealand Pty. Ltd.
1919 Malvern Road
Malvern East VIC 3145 Australia

Phone: +64 9 838 0276
Fax: +64 9 838 0275

Malaysia Office
Ultradata Malaysia Sdn. Bhd.
Unit 5-1, Level 5
Tower 9, Avenue 5, The Horizon,
Bangsar South
No.8, Jalan Kerinchi
59200 Kuala Lumpur, Malaysia

Phone: +60 3 3 2240 7767
Fax: +60 3 2283 1076

Disclaimer

Whilst every effort has been made to verify the accuracy of the information contained in this document, no responsibility is accepted by Ultradata Australia Pty Ltd for any loss suffered as a result of its application or use. This document is provided "as is" without warranty of any kind, express or implied, including, without limitation, the implied warranties of fitness for a particular purpose, merchantability or performance. In applying or using the information contained in this document you acknowledge that you do so at your own risk. In no event shall Ultradata Australia Pty Ltd be liable for any damages whatsoever, direct or indirect, including, damages for the loss of business profit, business interruption, loss of business information, or any other loss, arising from the use or application of the information contained in this document and, to the maximum extent permitted by law, disclaims all liability for any loss or damage (including consequential loss or damage) that may be suffered or incurred by you or any third party.

Whilst every reasonable effort has been made to ensure the accuracy of the information contained in this document if discrepancies exist between the user manual and the actual functionality it should be assumed that the functionality is correct. If you have any feedback on the contents or believe there are inaccuracies, please send an email to documentation@ultradata.com.au.

Table of Contents

Introduction

This document has been prepared by Ultradata Australia Pty. Ltd as a guide only. The information provided is intended to be used for general information and instruction purposes only and should not be considered a specific model for your financial institution's Fraud Monitor rules model. In applying or using the information contained in this document you acknowledge that that you do so at your own risk.

While every effort has been made to verify the accuracy of the information contained in this document, Ultradata makes no warranty as to the accuracy or reliability of the information provided in this document (which may vary at any time without notice) and, to the maximum extent permitted by law, disclaims all liability for any loss or damage (including consequential loss or damage) that may be suffered or incurred by as a result of the application or use of any information in this document (or anything omitted from the document). You must at all times indemnify and hold harmless Ultradata, its officers, employees and agents from and against all costs, expenses, losses and damages arising out of any claim by a third party arising from the application or use of any information in this document by you.

This document contains commercially sensitive information that should be treated as strictly confidential. No part of this document may be reproduced or distributed without the express written permission of Ultradata.

Who is this document for?

This manual has been designed for people who create rules for the Fraud Interceptor.

References

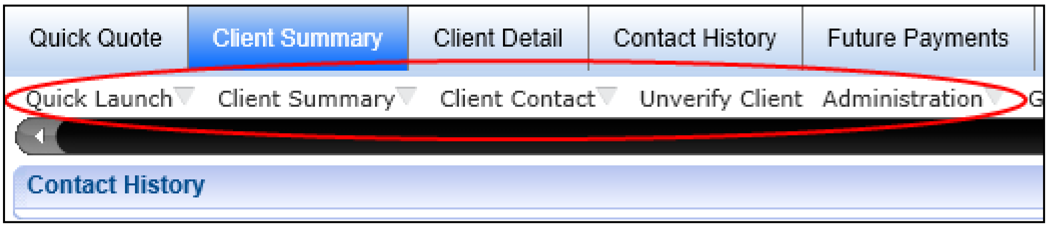
- *Fraud Interceptor User Manual*

Accessing the pages and programs in this manual

There are a number of ways to access the pages and programs described in this manual. The following methods are most frequently used within Ultracs:

Sliding Menu

The sliding menu is displayed above the main work area of Ultracs. It contains a list of menu items and may contain drop-down menus with further items.

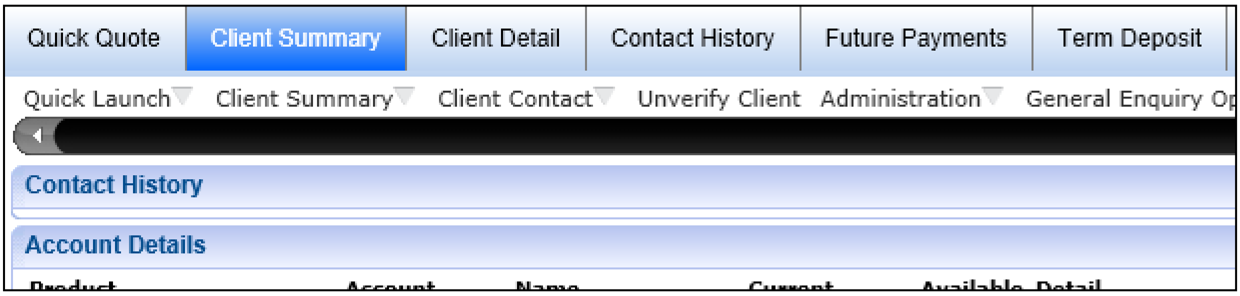


If there are more menu items that will fit across the screen, a slider is displayed. Move the slider (under the menu) if you cannot see the menu item you are looking for.

Your system administrator will most likely create menus for different groups of operators to give you quick access to a list of pages and programs that you most commonly use. To access a page or program from the sliding menu, simply click on the appropriate menu item, or in the case of a drop-down menu, extend the menu and then click on the appropriate item from this drop-down list. The corresponding page or program will open in the main working area of the screen.

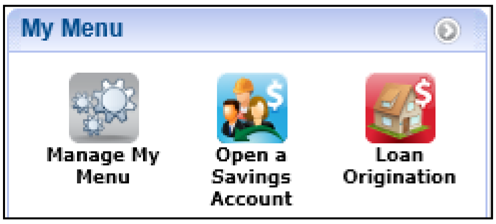
Tabbed Pages

Some products and functionality may present information in a series of tabbed pages.



In this example there are page tabs for Quick Quote, Client Summary, Client Detail, Contact History, Future Payments and Term Deposit. The Client Summary is the page currently selected and the tab is highlighted. The page tabs can be used to quickly move from one page to another. Click on the page tab to go to the page you want. Refer to the appropriate manual for the product in question.

My Menu

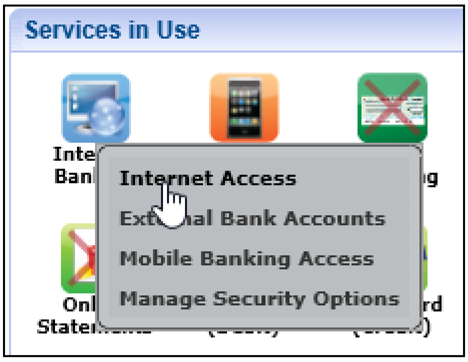


The **My Menu** widget can be found on the right-hand side of the Ultracs main menu.

You are able to add to this widget any pages or programs that you commonly use and would like to access quickly by using the **Manage My Menu** icon.

See the *Getting Started in Ultracs User Manual* for information on this feature.

Services in Use



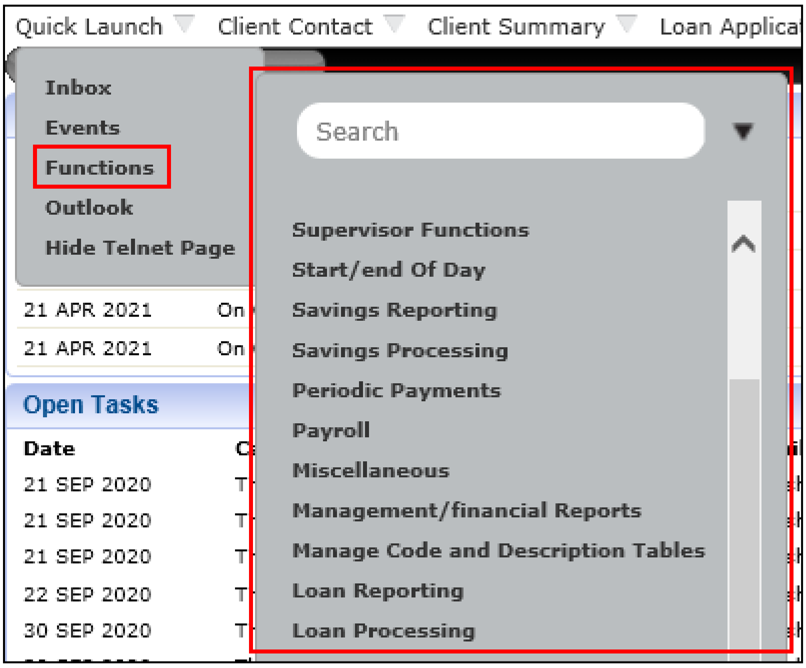
The **Services in Use** widget contains a number of icons for different services (or products) that may be available to a client. This widget is only displayed when a client is 'in focus'. Click on any of the services icons to view a pop-up menu of pages, programs and functions related to the service.

See the *Getting Started in Ultracs User Manual* for information on this feature.

Functions Menu

The **Functions** menu is accessed by clicking on the 'Quick Launch' drop-down menu item on the sliding menu and then selecting **Functions**. The menus displayed are dependent on your individual settings.

From this menu, you can access programs via the Ultracs 'Telnet Hosting' function and front-end pages that have been converted from host-based programs.



Rules and Responses

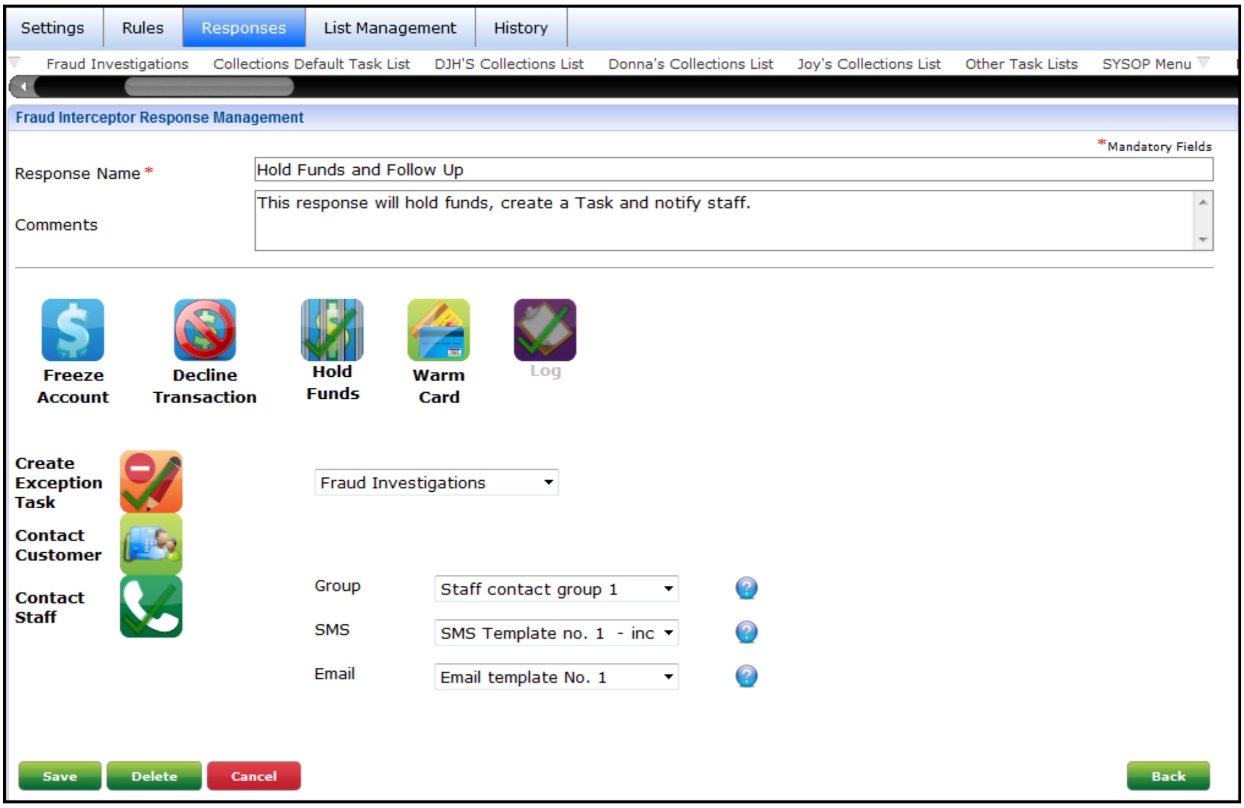
Fraud can take many forms and there is no definitive means of detection and prevention that can cover all of its variations. Ultradata's Fraud Interceptor is a monitoring tool that analyses transactions passing through the Ultracs core banking system and is based on a system of Rules and statistical analysis that can start a case management workflow for monitoring and disabling suspicious transactions.

Once a Rule triggers the processing of a suspicious transaction, a Response is generated. The Response is the action taken. For example, it could be sending a message to the client, declining a transaction, freezing an account or some other action.

Events and Tasks are generated as appropriate for the Response and details are recorded against the Client History and are also passed through to the Reporting Database for use with the generation of standard or customised reports.

Responses

Fraud Responses initiate the action to be taken when a Rule is triggered by a suspect transaction. Ideally, you should set up the appropriate Responses and Actions prior to creating your Fraud Interceptor Rules.



Fraud Interceptor Response Management

*Mandatory Fields

Response Name * Hold Funds and Follow Up

Comments This response will hold funds, create a Task and notify staff.

Fraud Investigations

Group Staff contact group 1

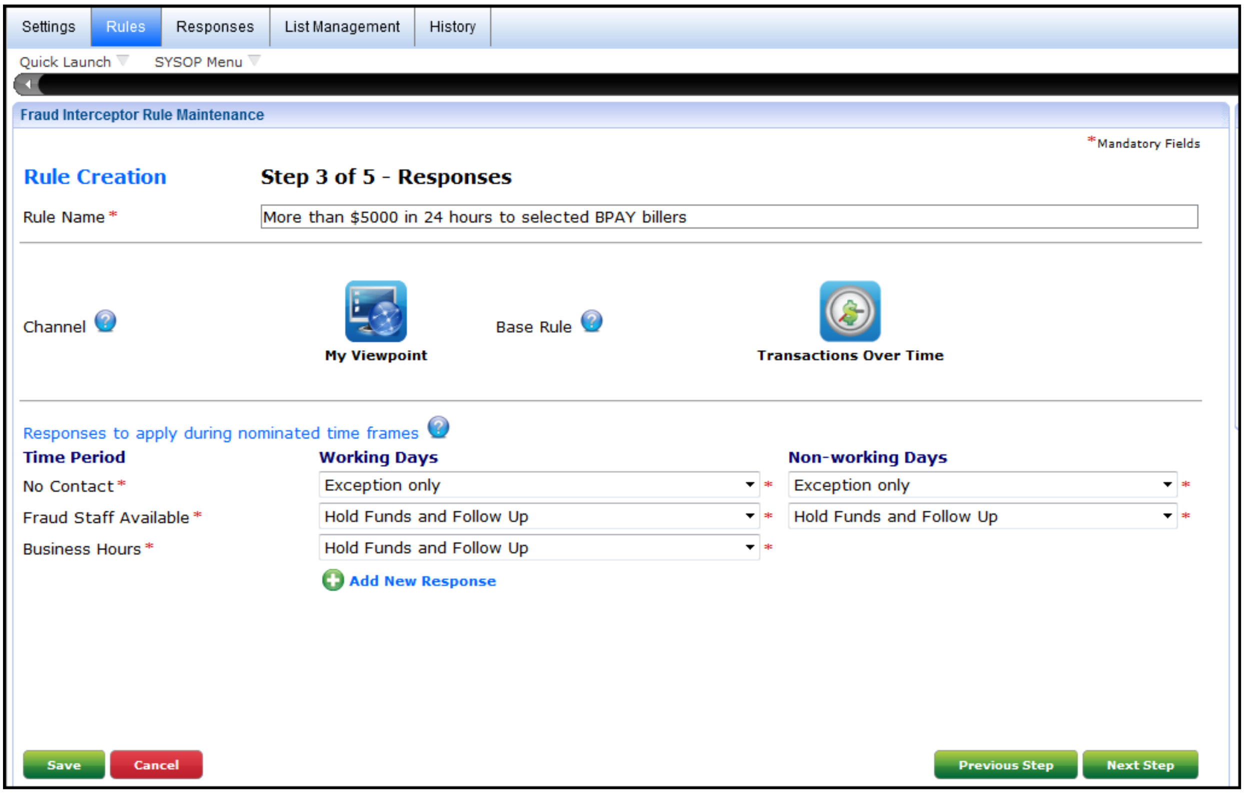
SMS SMS Template no. 1 - inc

Email Email template No. 1

The actions that may be taken could include one or more of the following:

- Freeze Account
- Decline Transaction
- Hold Funds
- Warm Card
- Create Exception Task
- Contact Customer
- Contact Staff
- All Responses will include recording the action into the Fraud Interceptor Log.

Responses are linked to Rules in Step 3 of the Rule Creation process:



*Mandatory Fields

Rule Creation **Step 3 of 5 - Responses**

Rule Name * More than $5000 in 24 hours to selected BPAY billers

Channel: My Viewpoint

Base Rule: Transactions Over Time

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact *	Exception only *	Exception only *
Fraud Staff Available *	Hold Funds and Follow Up *	Hold Funds and Follow Up *
Business Hours *	Hold Funds and Follow Up *	

It is up to your institution to determine the appropriate Response according to the perceived risk in line with your overall risk management strategy. Unless a specific Response is integral to the Rule, Responses are not shown in this manual. Detailed information on how to set up Responses and how to integrate them into the Rules is provided in the *Fraud Interceptor User Manual*.

Fraud Interceptor Rules - Examples

This manual provides a number of example rules, based on scenarios, for use with the Fraud Interceptor. The rules can be used as a guide to help you understand how to create the rules you will set up and use with the Fraud Interceptor.

Only the key fields and settings are explained in this manual. In most examples, this only includes selected fields and settings from Steps 1 and 2. The options entered for all other Steps are essentially the same, according to your financial institution's requirements, and are not specific to individual scenarios. For detailed information on all fields in the five-step rule creation process and how rules are used within the Fraud Interceptor, refer to the *Fraud Interceptor User Manual*.

Note that the rules shown in these examples are grouped by channel. Some of these rules may be created for more than one channel, for example a rule using the Geographic Impossibility base rule may be created for ATM, EFTPOS, VISA or Bank@Post channels; however; you cannot create a Geographic Impossibility rule for 'All Channels'. This means that if you want a Geographic Impossibility rule for each of these channels, you will need to create four rules. The Fraud Interceptor Rules page lets you copy existing rules and change the channel, which means once you create the first rule; it will not take very long to create the other three.

VISA Channel Rules

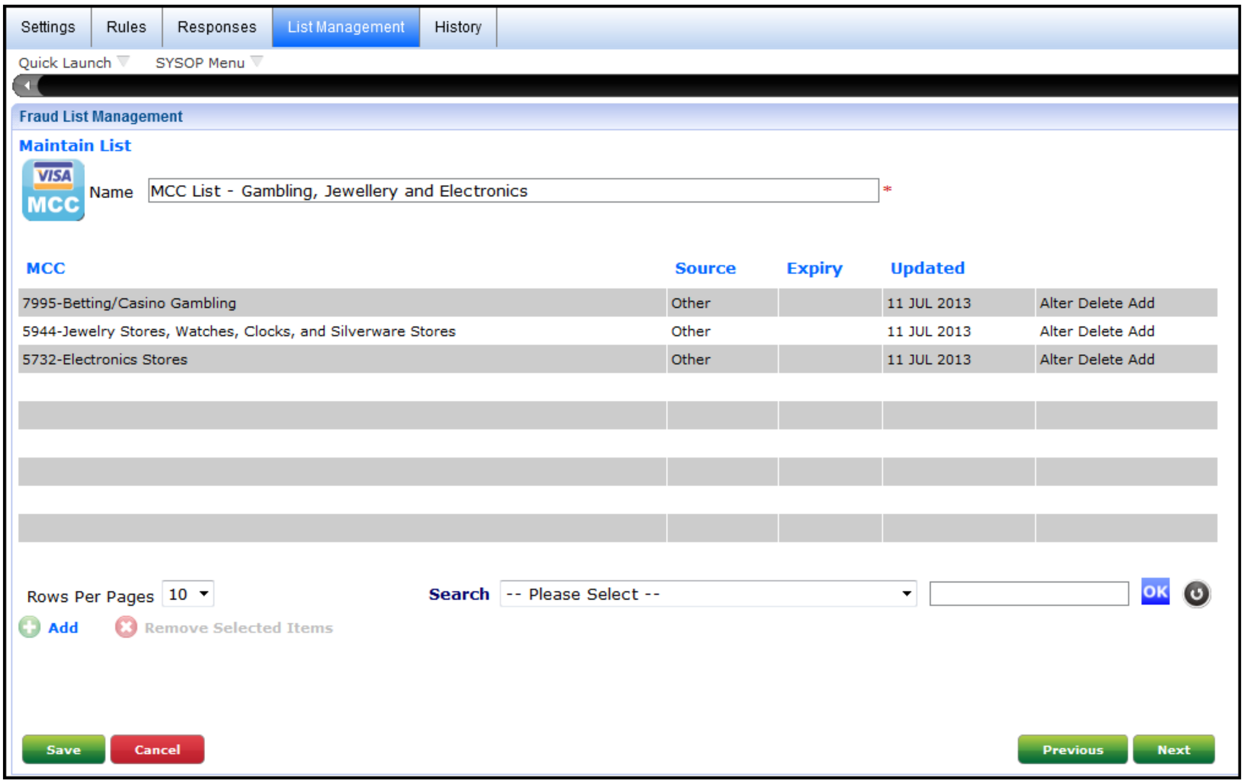
The following examples cover a number of scenarios that may be useful for monitoring VISA card transactions.

- Sum of VISA transactions exceeds $5,000 in 24 hours at specific MCCs - Gambling, Jewellery and Electronics
- More than four transactions to specific countries in 24 hours
- Card not present transactions of $5,000 or more
- More than four card present transactions in 24 hours to the same merchant for specified MCCs
- Any transaction for MCC 7995 (Gambling) greater than $500
- Any foreign VISA transaction greater than $10,000
- Any transaction from specific merchants identified as points of concern
- VISA - iTunes/Apple, overseas transactions
- VISA - Any transactions to selected Russian/Eastern European countries
- VISA - Low value transaction followed by a high value transaction
- VISA - More than three VISA manual or unspecified source transactions (Card Number Entry)
- VISA - Card rejection codes

Sum of VISA transactions exceeds $5,000 in 24 hours at specific MCCs - Gambling, Jewellery and Electronics

This rule is triggered when the sum of VISA transactions exceeds a specified value within 24 hours for transactions for specified merchant categories. Before creating this rule, you need to create a Merchant Category Code (MCC) list which contains the appropriate category codes.

Fraud List Management



Name MCC List - Gambling, Jewellery and Electronics *

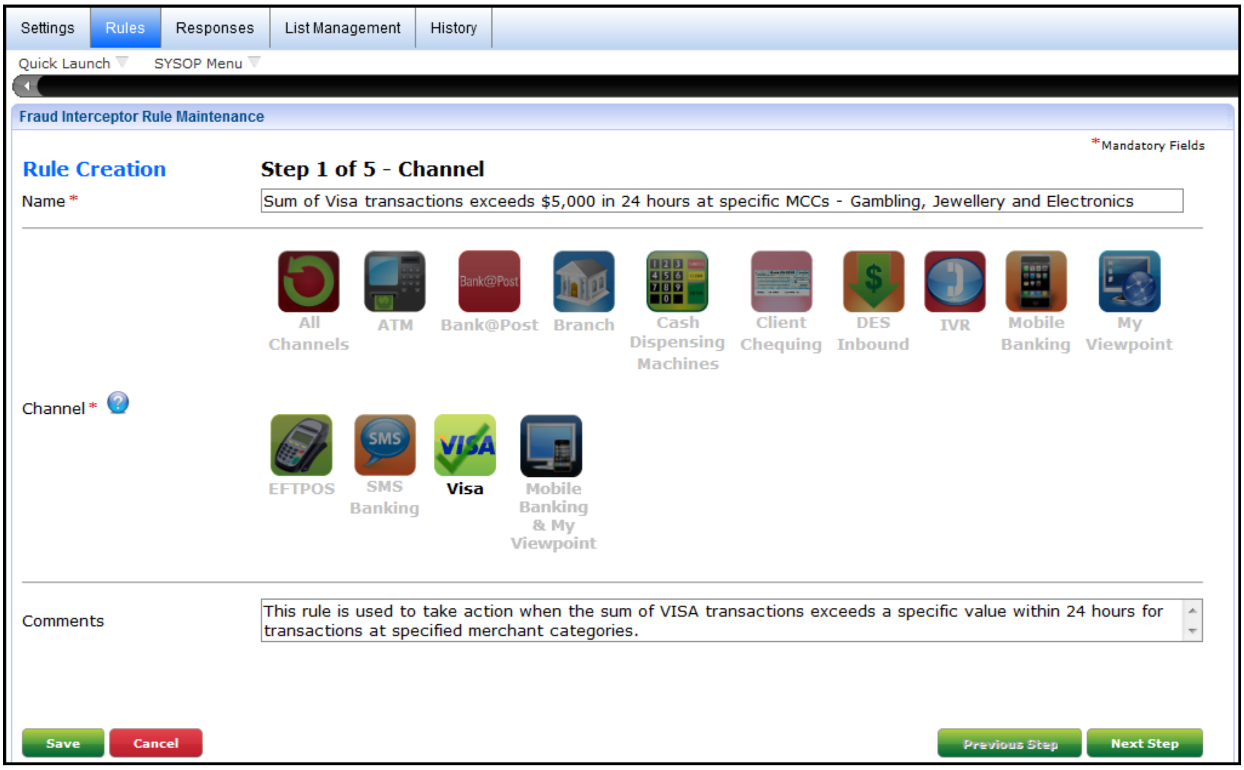
MCC	Source	Expiry	Updated	
7995-Betting/Casino Gambling	Other		11 JUL 2013	Alter Delete Add
5944-Jewelry Stores, Watches, Clocks, and Silverware Stores	Other		11 JUL 2013	Alter Delete Add
5732-Electronics Stores	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages 10

Search -- Please Select --

This List contains entries for Gambling (7995), Jewellery (5944) and Electronics (5732).

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel

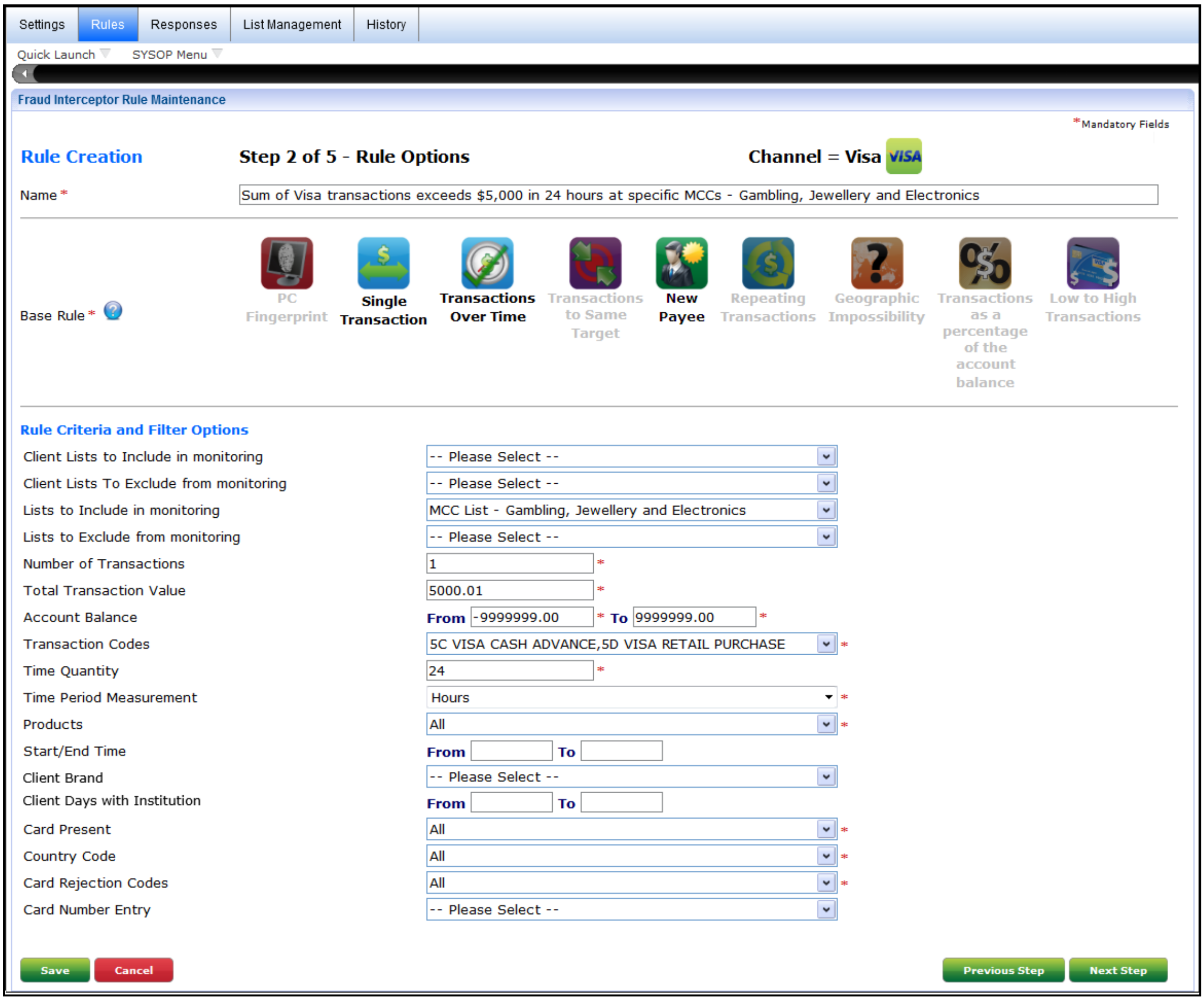


Name * Sum of Visa transactions exceeds $5,000 in 24 hours at specific MCCs - Gambling, Jewellery and Electronics

Comments: This rule is used to take action when the sum of VISA transactions exceeds a specific value within 24 hours for transactions at specified merchant categories.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation Step 2 of 5 - Rule Options Channel = Visa

Name * Sum of Visa transactions exceeds $5,000 in 24 hours at specific MCCs - Gambling, Jewellery and Electronics

Base Rule * Transactions Over Time

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	MCC List - Gambling, Jewellery and Electronics
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	1 *
Total Transaction Value	5000.01 *
Account Balance	From -9999999.00 * To 9999999.00 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	The MCC List you created for this rule has been selected from the drop-down list 'Lists to Include in monitoring'. A client list (Include or Exclude) is optional and if both Include and Exclude lists are left unselected, all matches will be included in this rule. 'Lists to Exclude from monitoring' should be left as "-- Please Select --".
Number of Transactions	If you enter '1' into this field, any number of transactions will be considered.
Total Transaction Value	As this rule is to apply to the sum of transactions over $5,000 and the field itself will include the value entered, you need to enter 5000.01 (or 5001 if you are not concerned with cents).
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.

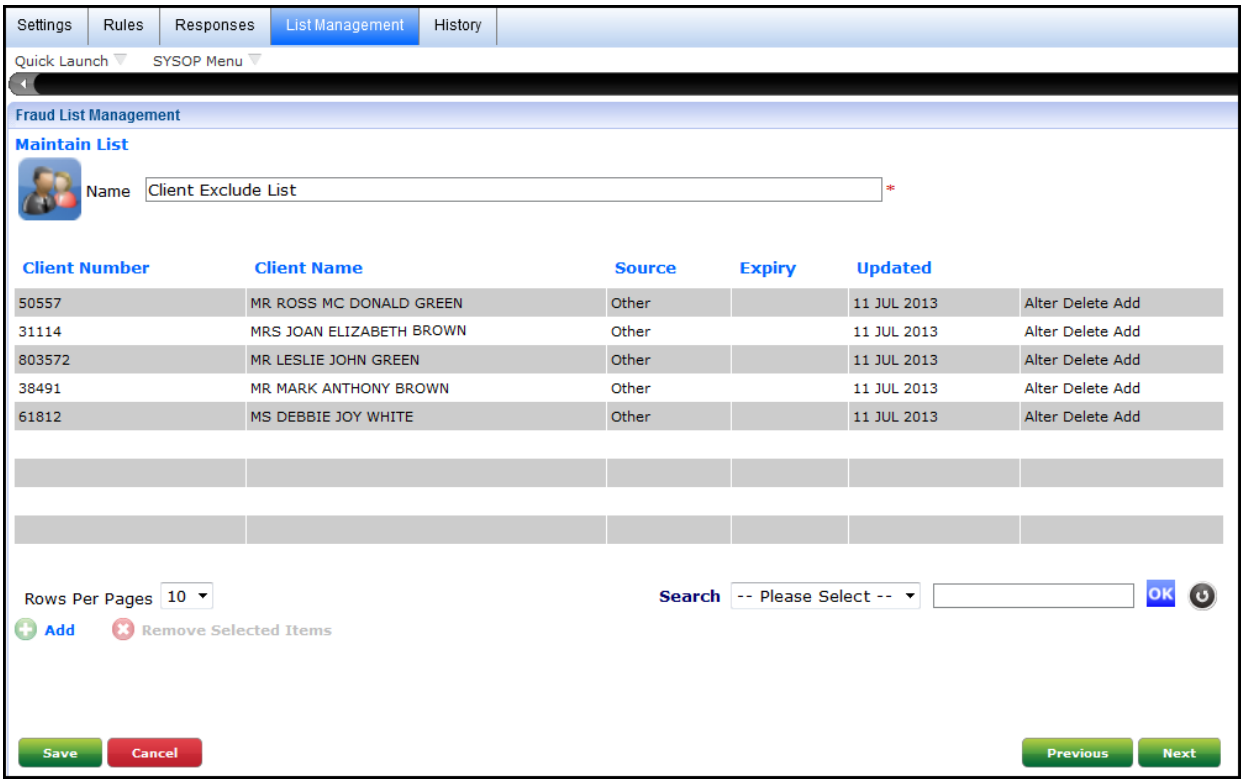
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. The minimum you are likely to require are VISA Cash Advance and VISA Retail Purchase codes. You may also include other codes, such as ATM/POS Withdrawal, if you consider those codes appropriate.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected, however you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By selecting 'All' you are catering for personal transactions as well as telephone and Internet transactions.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

More than four transactions to specific countries in 24 hours

This rule is triggered when a set number of VISA transactions occur within 24 hours in any of the countries specified. Before creating this rule, you may need to create a Client List to exclude known low-risk clients from monitoring.

> In this scenario, it does not matter which of the countries are included in the count of four transactions. If you want the rule to apply to four transactions from the same country, then you will need to create a separate rule for each country.

Fraud List Management



Maintain List

Name: Client Exclude List *

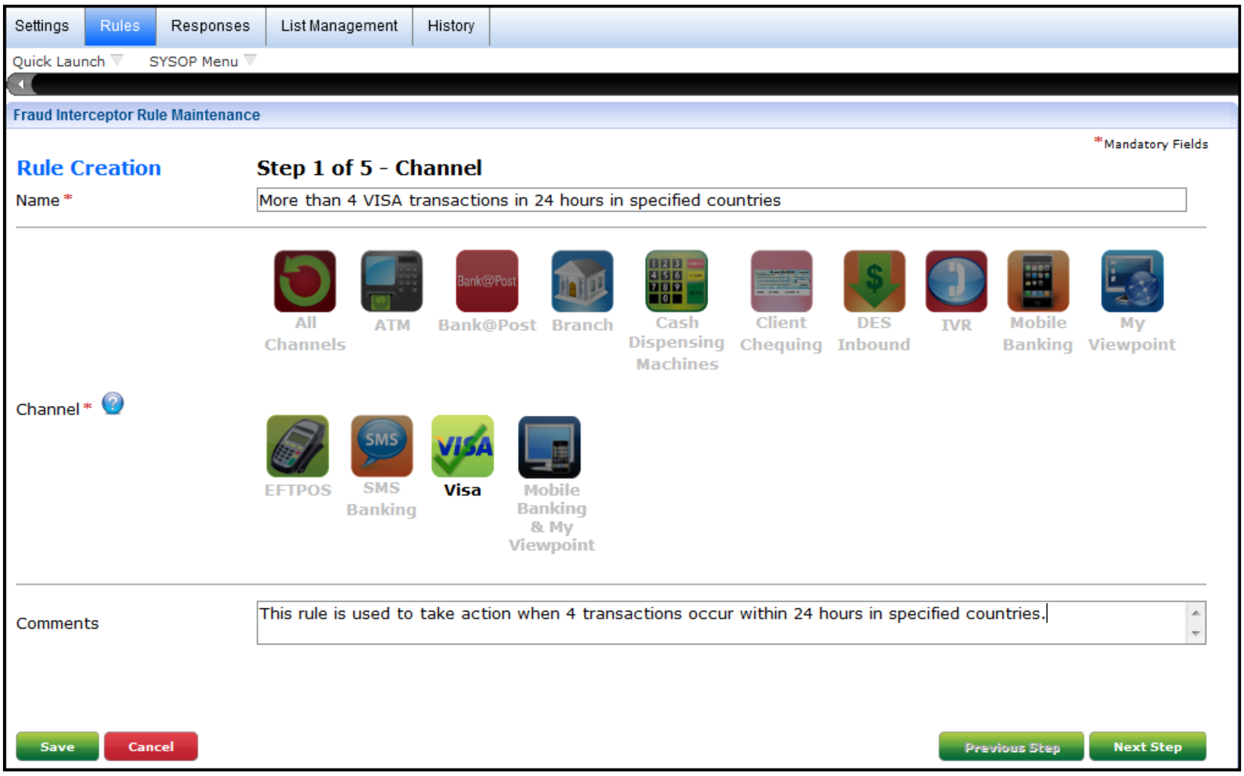
Client Number	Client Name	Source	Expiry	Updated	
50557	MR ROSS MC DONALD GREEN	Other		11 JUL 2013	Alter Delete Add
31114	MRS JOAN ELIZABETH BROWN	Other		11 JUL 2013	Alter Delete Add
803572	MR LESLIE JOHN GREEN	Other		11 JUL 2013	Alter Delete Add
38491	MR MARK ANTHONY BROWN	Other		11 JUL 2013	Alter Delete Add
61812	MS DEBBIE JOY WHITE	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

The Client Exclude List contains the details of clients who will not be included in this rule. You can use this List to cater for known low-risk clients travelling to high-risk areas on a temporary basis by adding an Expiry date.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Rule Creation

Step 1 of 5 - Channel

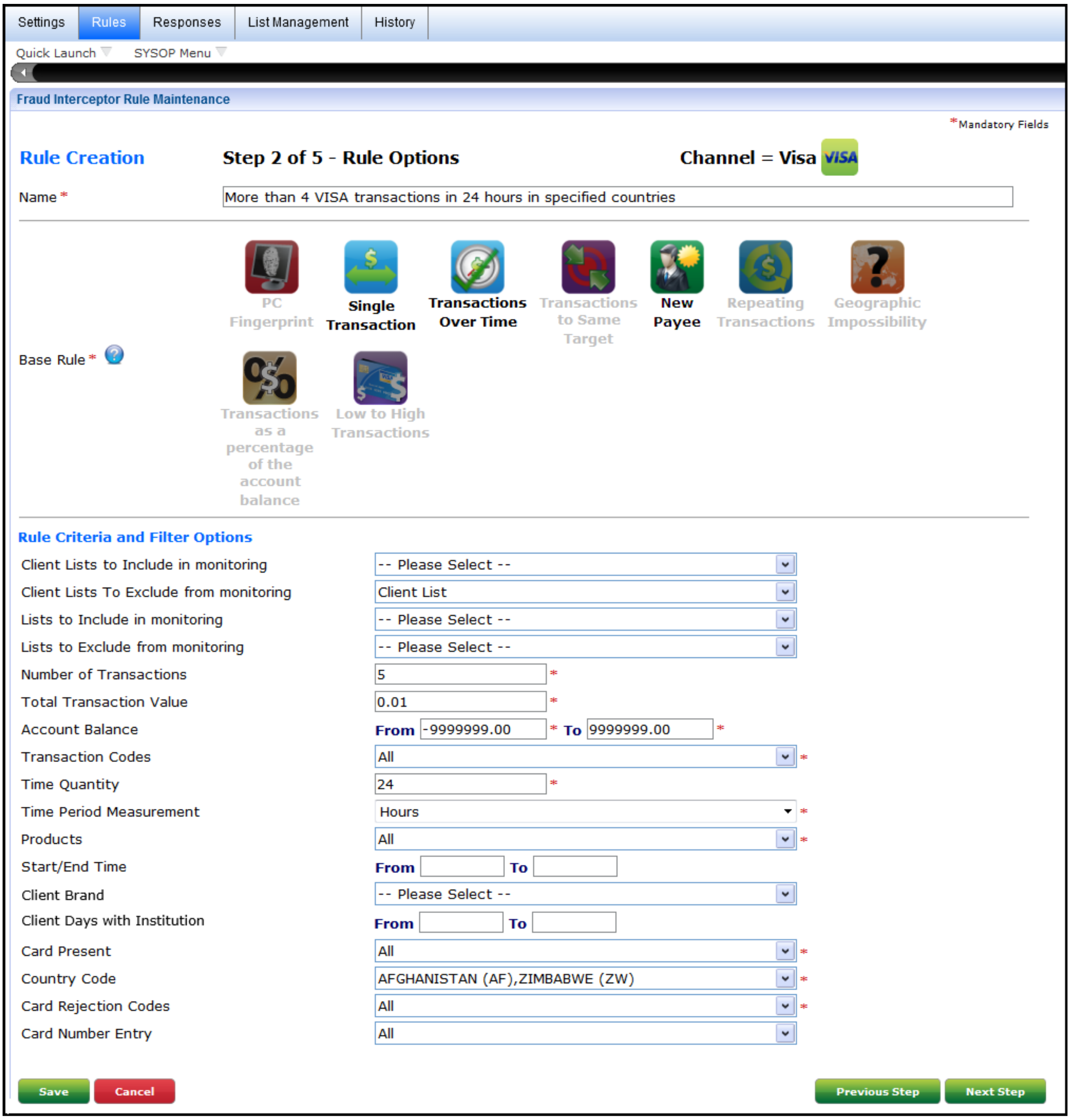
Name *: More than 4 VISA transactions in 24 hours in specified countries

Channel *: Visa

Comments: This rule is used to take action when 4 transactions occur within 24 hours in specified countries.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Visa**

Name * More than 4 VISA transactions in 24 hours in specified countries

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Client List
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	5 *
Total Transaction Value	0.01 *
Account Balance	From -9999999.00 * To 9999999.00 *
Transaction Codes	All *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	AFGHANISTAN (AF),ZIMBABWE (ZW) *
Card Rejection Codes	All *
Card Number Entry	All

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	You can optionally exclude known 'safe' clients. This has been done by selecting the "Client Exclude List" from the 'Client Lists to Exclude from Monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --".
Number of Transactions	The scenario is triggered when '5' transactions occur within the specified time frame.

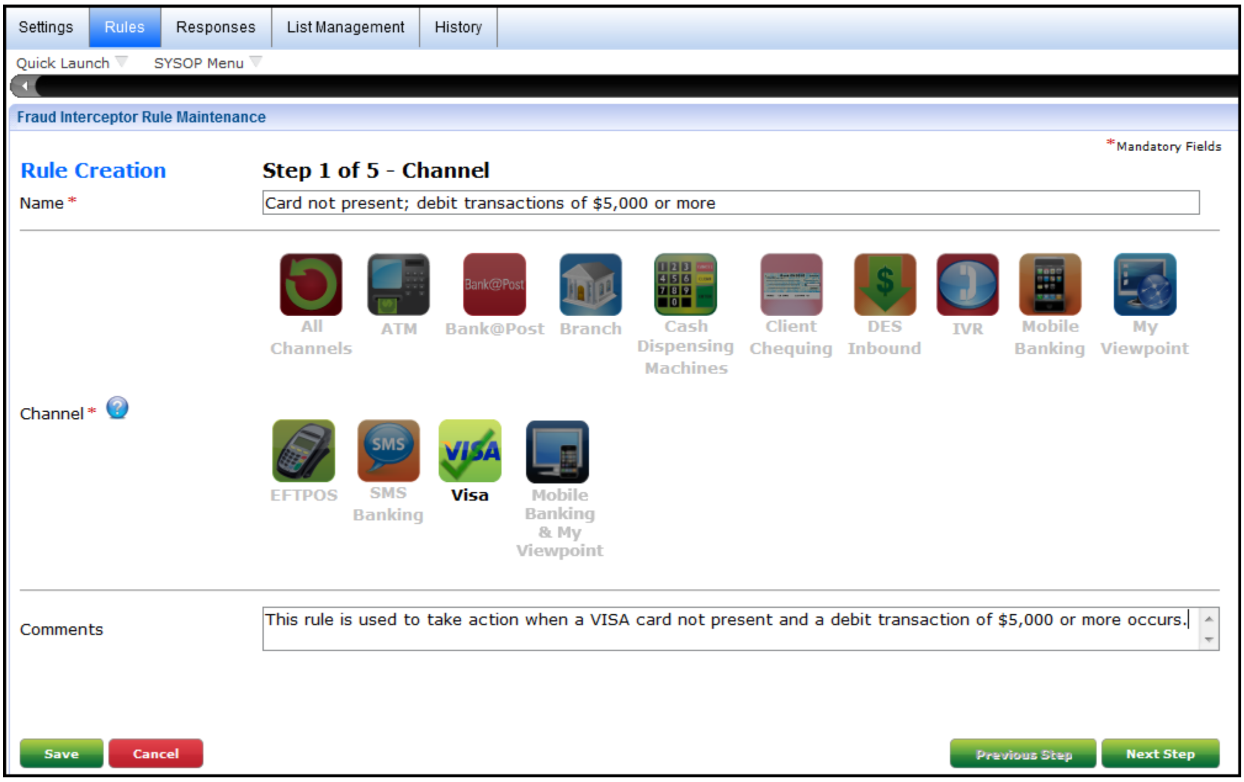
Total Transaction Value	Any value of the transactions should be allowed to trigger this scenario; however, it is unlikely they will have a negative overall total so you may as well enter 0.01.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	You can either select appropriate transaction codes relating to the type of transaction likely to occur (e.g. VISA Cash Advance, VISA Retail Purchase and various ATM transactions). In this example, 'All' has been selected, however, if you don't want credit and fee transactions to be included, you will need to select the specific transaction codes.
Time Quantity **Time Period Measurement**	These two fields are used together, and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected; however, you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By selecting 'All' you are catering for personal transactions as well as telephone and Internet transactions.
Country Code	Select the countries you require from the drop-down list. In this example, two countries have been selected.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. In this example, 'All' has been selected to include all card number entry methods.

Card not present transactions of $5,000 or more

This rule is triggered by a VISA 'card not present' transaction of $5,000 or more.

Before creating this rule, you may need to create a Client List to exclude known low-risk clients from monitoring.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Step 1 of 5 - Channel

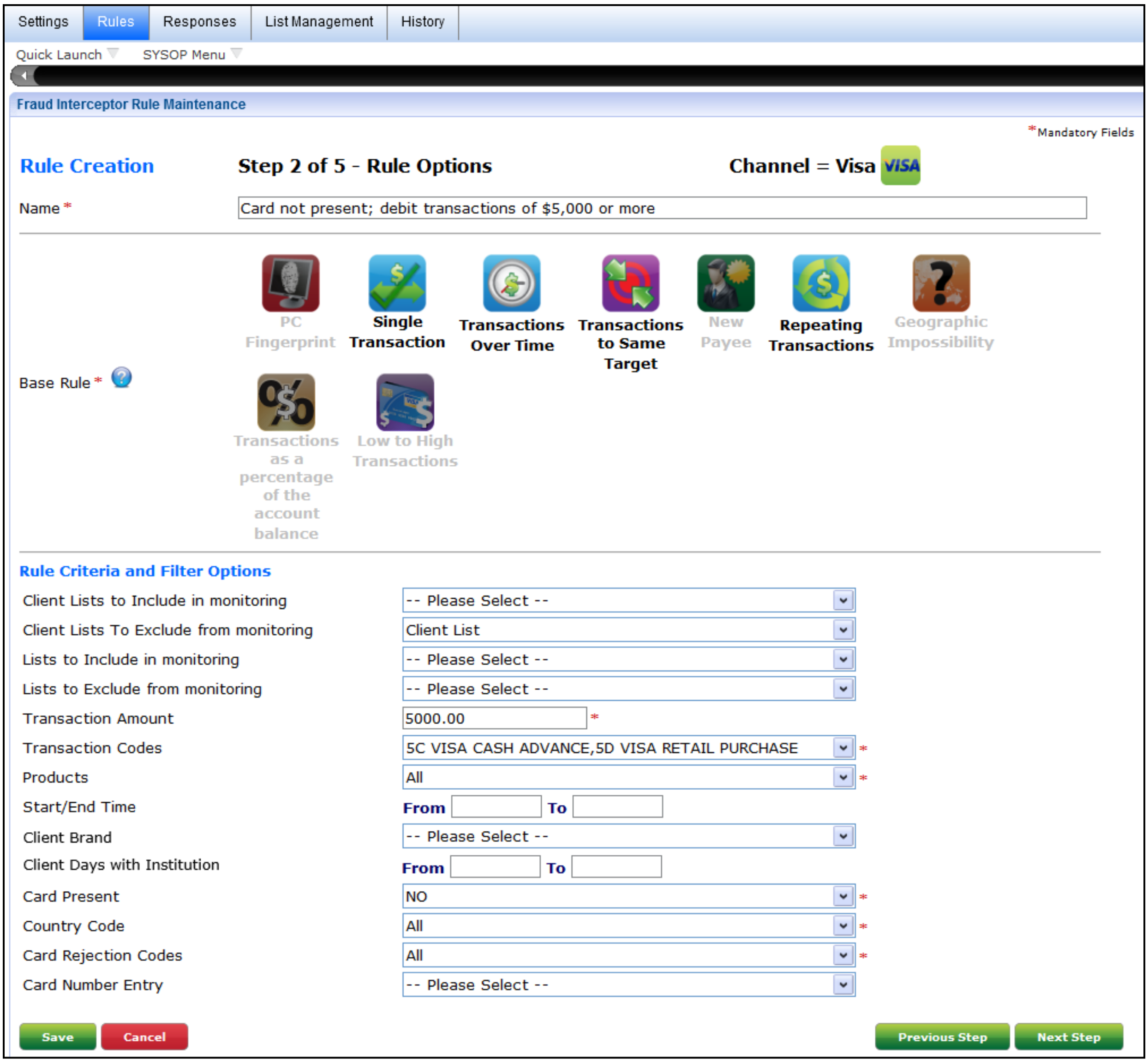
Name * Card not present; debit transactions of $5,000 or more

Channel * Visa

Comments This rule is used to take action when a VISA card not present and a debit transaction of $5,000 or more occurs.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation — Step 2 of 5 - Rule Options — Channel = Visa

Name * : Card not present; debit transactions of $5,000 or more

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Client List
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	5000.00 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	NO *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Single Transaction'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	You can optionally exclude known 'safe' clients. This has been done by selecting the "Client Exclude List" from the 'Client Lists to Exclude from Monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --".
Transaction Amount	This rule is to be triggered by a single transaction of $5000 or more so '5000.00' is entered into this field.

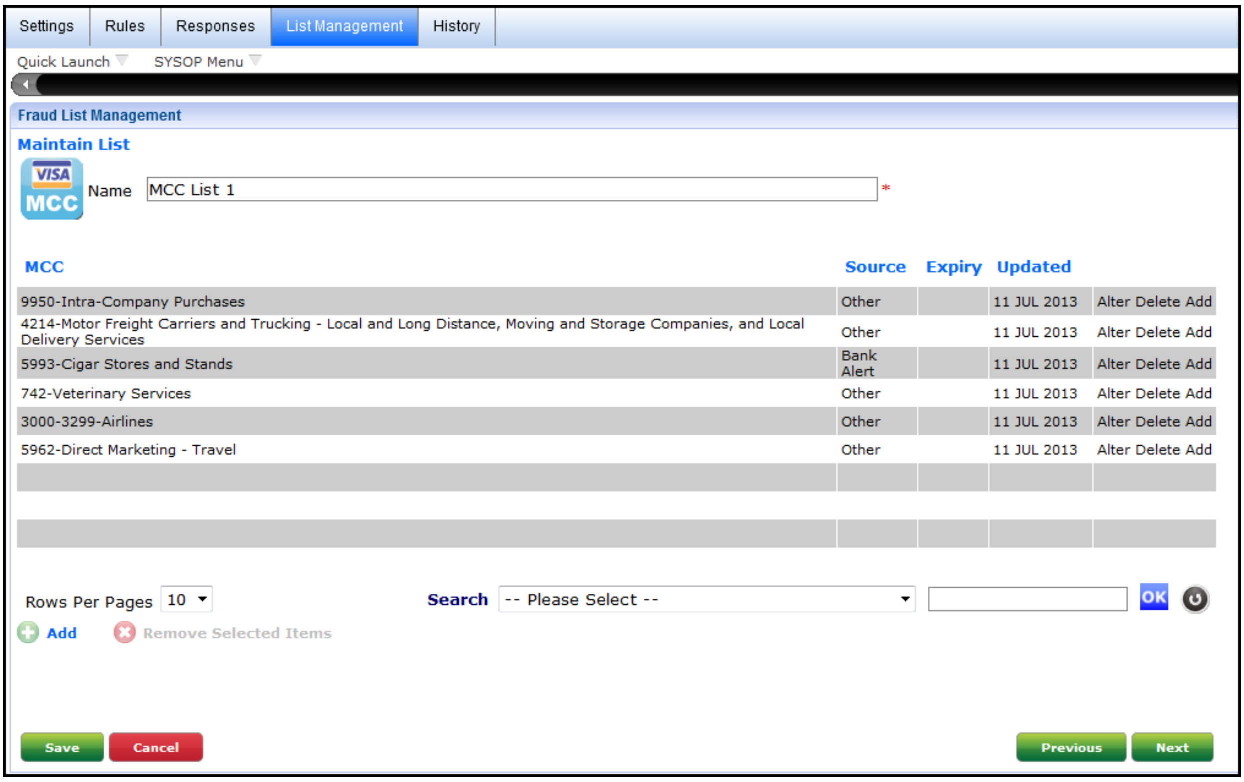
Transaction Codes	This rule only applies to VISA debit transactions where a card is not present; therefore, you can ignore ATM and POS transaction. Select VISA Cash Advance and VISA Retail Purchase from the list of transaction cards.
Products	'All' has been selected, however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	This field must be set to 'NO' as only card not present transactions are to be considered.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example (as the absence of the card is covered by the Card Present criteria).

More than four card present transactions in 24 hours to the same merchant for specified MCCs

This rule is triggered when four or more card debit transactions occur within 24 hours to the same merchant for any merchants in one or more specified MCC Lists. The MCC Lists must be set up before creating the rule.

Fraud List Management

A MCC list will be required for this rule unless the rule will be applied to all merchants. The following shows an example of an MCC list.



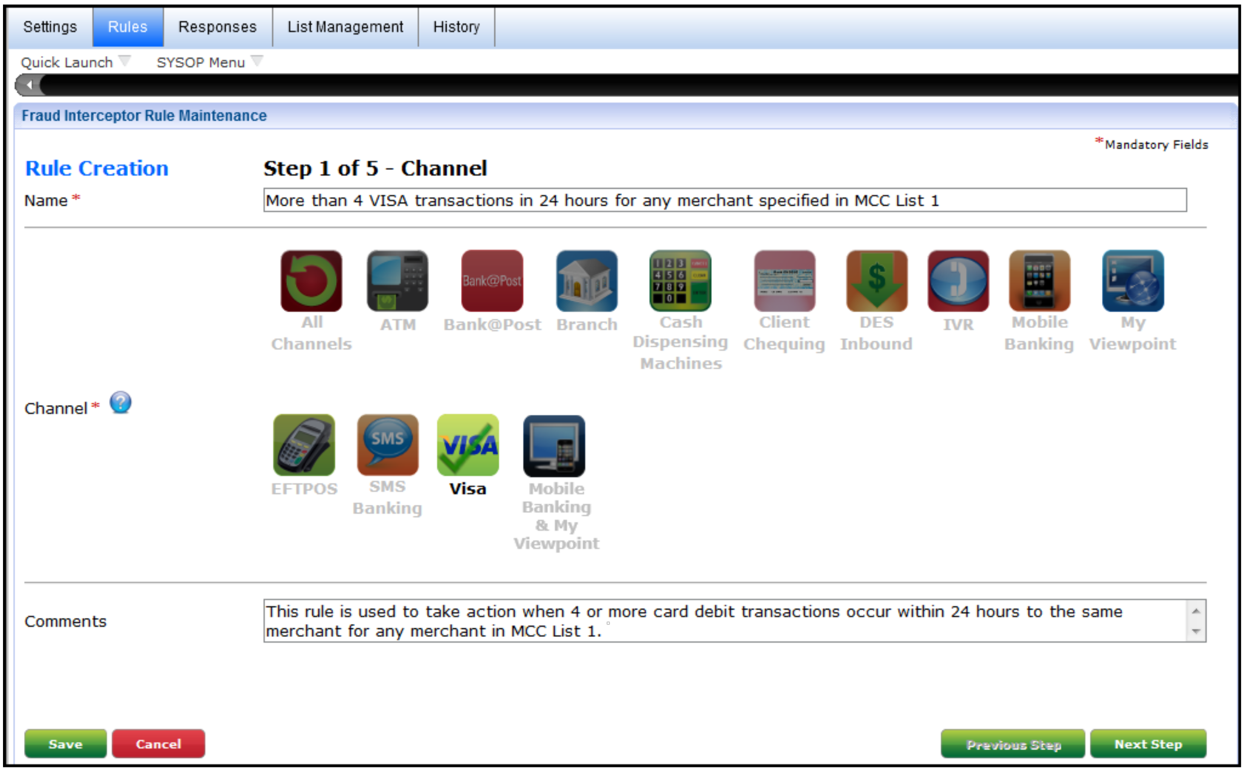
Name: MCC List 1 *

MCC	Source	Expiry	Updated	
9950-Intra-Company Purchases	Other		11 JUL 2013	Alter Delete Add
4214-Motor Freight Carriers and Trucking - Local and Long Distance, Moving and Storage Companies, and Local Delivery Services	Other		11 JUL 2013	Alter Delete Add
5993-Cigar Stores and Stands	Bank Alert		11 JUL 2013	Alter Delete Add
742-Veterinary Services	Other		11 JUL 2013	Alter Delete Add
3000-3299-Airlines	Other		11 JUL 2013	Alter Delete Add
5962-Direct Marketing - Travel	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Rule Creation

Step 1 of 5 - Channel

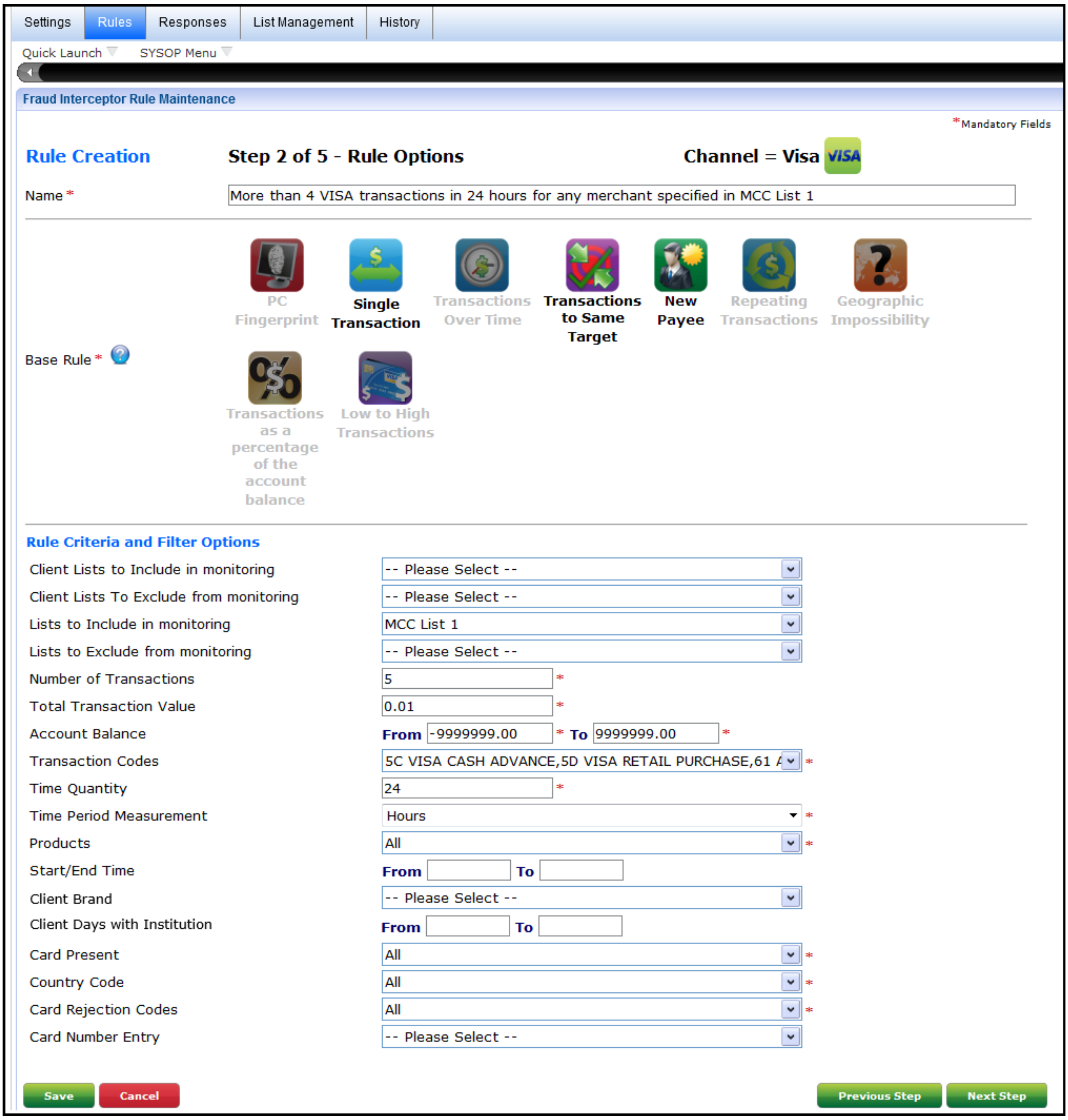
Name *: More than 4 VISA transactions in 24 hours for any merchant specified in MCC List 1

Channel *: Visa

Comments: This rule is used to take action when 4 or more card debit transactions occur within 24 hours to the same merchant for any merchant in MCC List 1.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation — **Step 2 of 5 - Rule Options** — **Channel = Visa**

Name * More than 4 VISA transactions in 24 hours for any merchant specified in MCC List 1

Base Rule * Transactions to Same Target

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	MCC List 1
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	5 *
Total Transaction Value	0.01 *
Account Balance	From -9999999.00 * To 9999999.00 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE,61 A *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Transactions to Same Target'.

The following criteria and filter options have been specified:

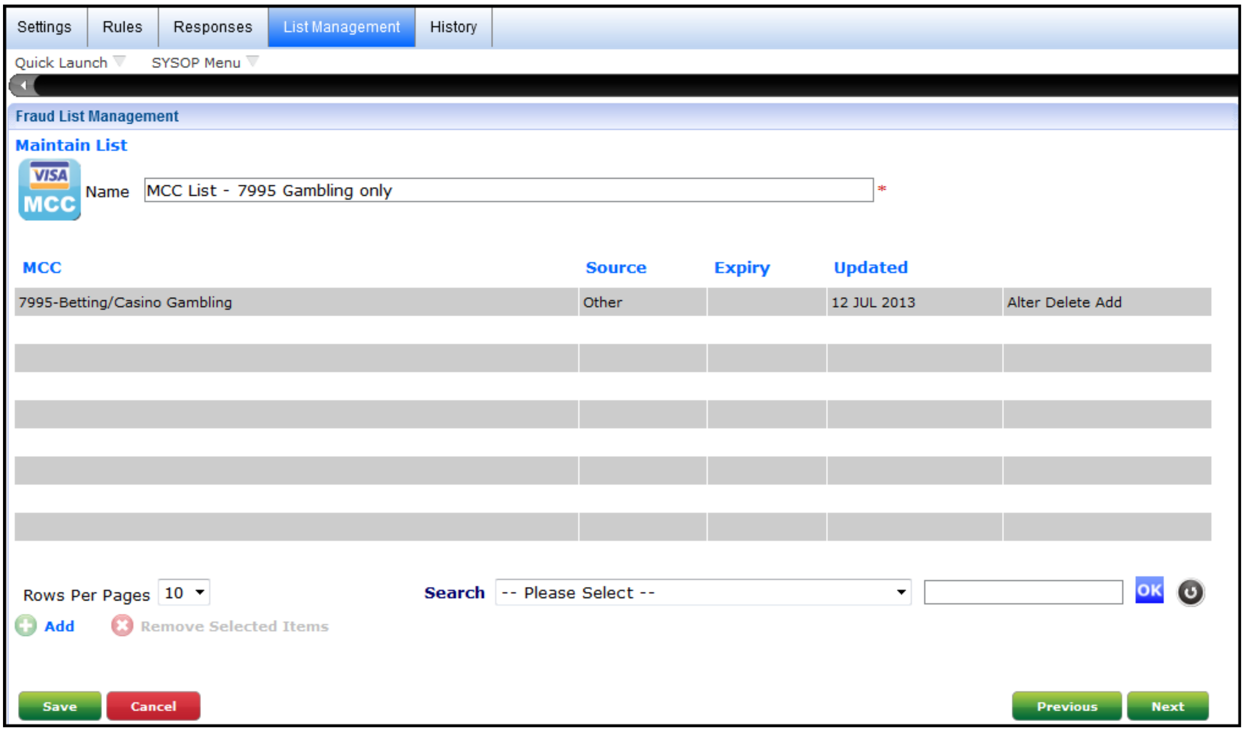
Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	Select the MCC List you created for this rule from the 'Lists to Include in monitoring' drop-down list. 'Lists to Exclude from monitoring' should be left as "-- Please Select --". A client list (Include or Exclude) is optional and if both are left unselected, all clients will be included in this rule.
Number of Transactions	The scenario is triggered when '5' (i.e. more than 4) transactions occur within the specified time frame.

Total Transaction Value	Any value of the transactions should be allowed to trigger this scenario; however, it is unlikely they will have a negative overall total so you may as well enter 0.01.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate transaction codes relating to the type of transaction likely to occur (e.g. VISA Cash Advance, VISA Retail Purchase). You may also select other transactions if you consider them appropriate, e.g. ATM/POS Withdrawal if this rule is to cover VISA Debit Cards using the 'debit' mode on a POS terminal. You cannot use the 'All' option as this would include credit transactions as well as debit transactions.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected; however, you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	This field must be set to 'YES' as only card present transactions are to be considered.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

Any transaction for MCC 7995 (Gambling) greater than $500

This rule is triggered when any VISA transaction for MCC 7995 (Gambling) is greater than $500. Before creating this rule, you will need to create a MCC type Fraud List that contains only merchants belonging to the gambling Merchant Category Code.

Fraud List Management



Fraud List Management

Maintain List

Name: MCC List - 7995 Gambling only *

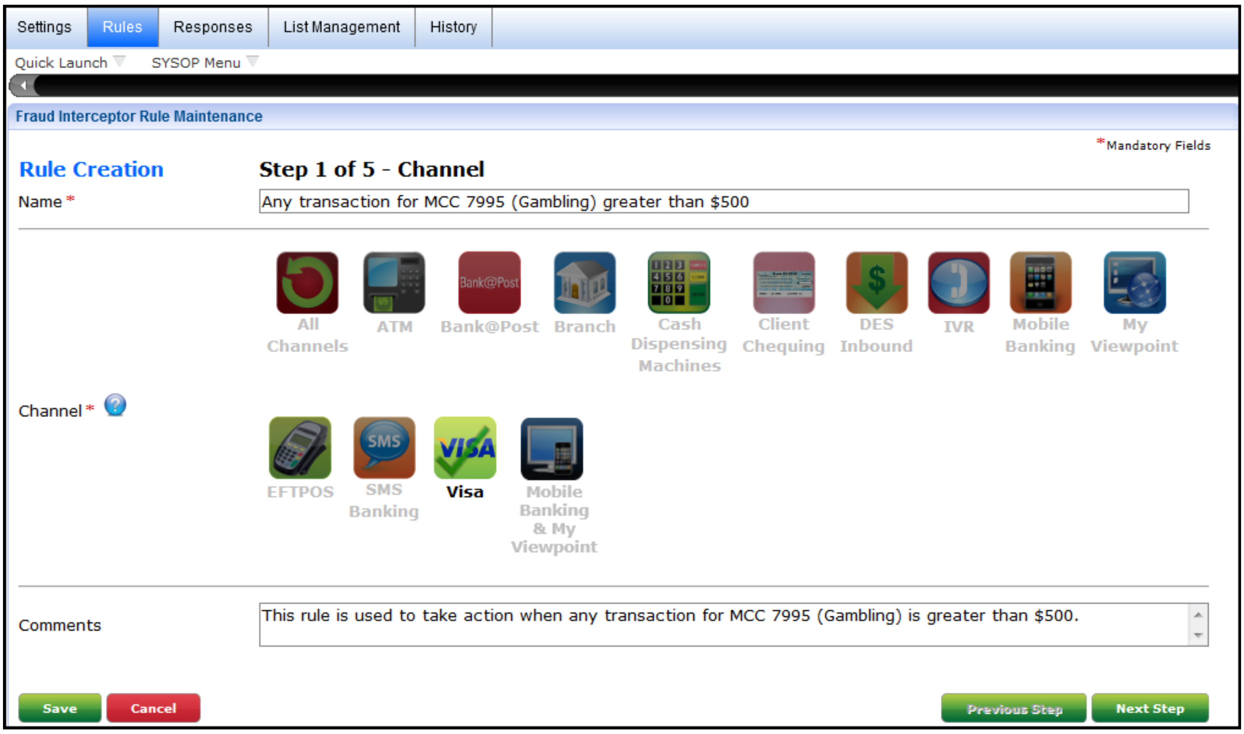
MCC	Source	Expiry	Updated	
7995-Betting/Casino Gambling	Other		12 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

This List contains only one entry for Gambling (7995).

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

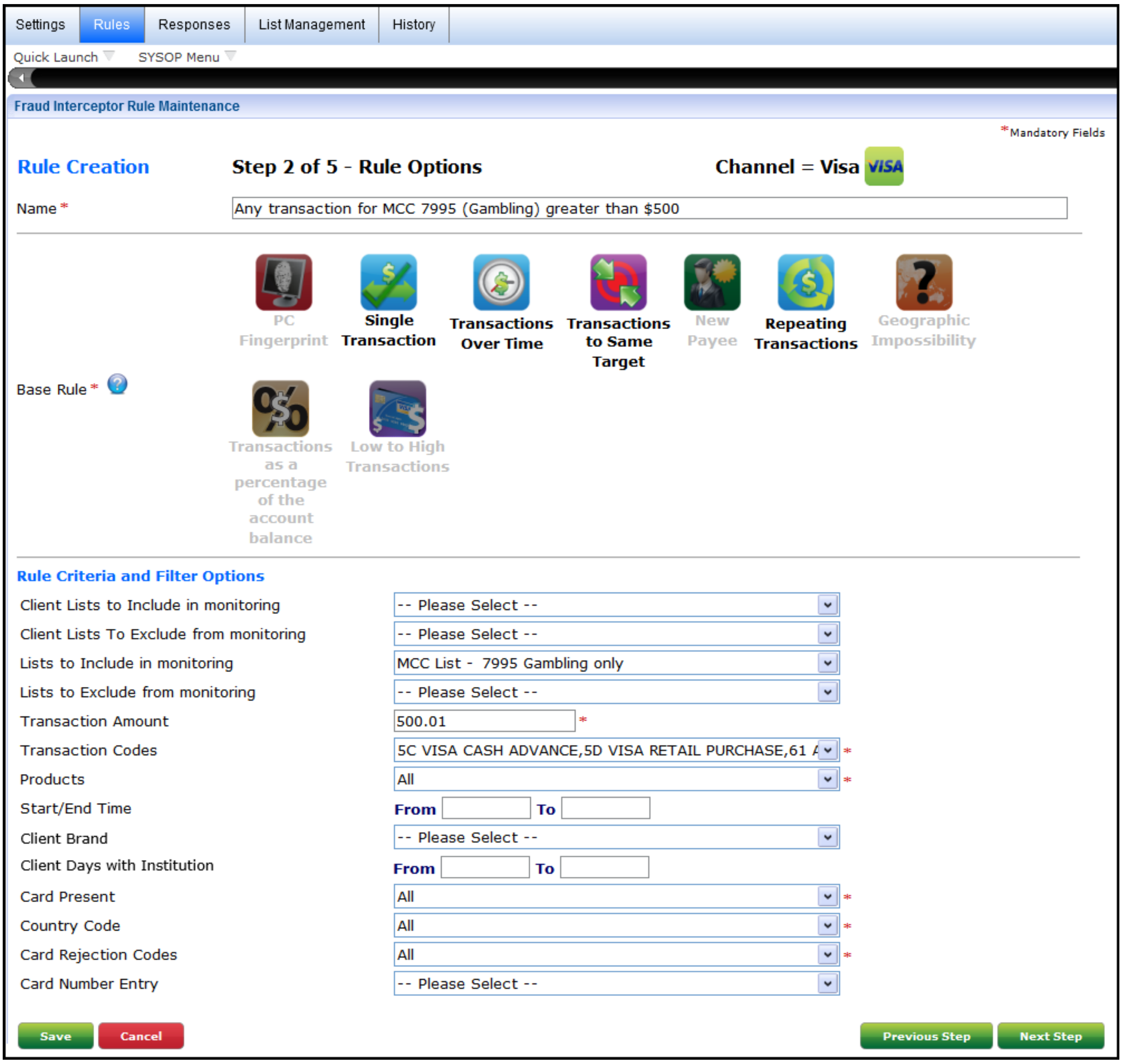
Name *: Any transaction for MCC 7995 (Gambling) greater than $500

Channel *: Visa

Comments: This rule is used to take action when any transaction for MCC 7995 (Gambling) is greater than $500.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation Step 2 of 5 - Rule Options Channel = Visa

Name * Any transaction for MCC 7995 (Gambling) greater than $500

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	MCC List - 7995 Gambling only
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	500.01 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE,61 A *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Single Transaction'.

The following criteria and filter options have been specified:

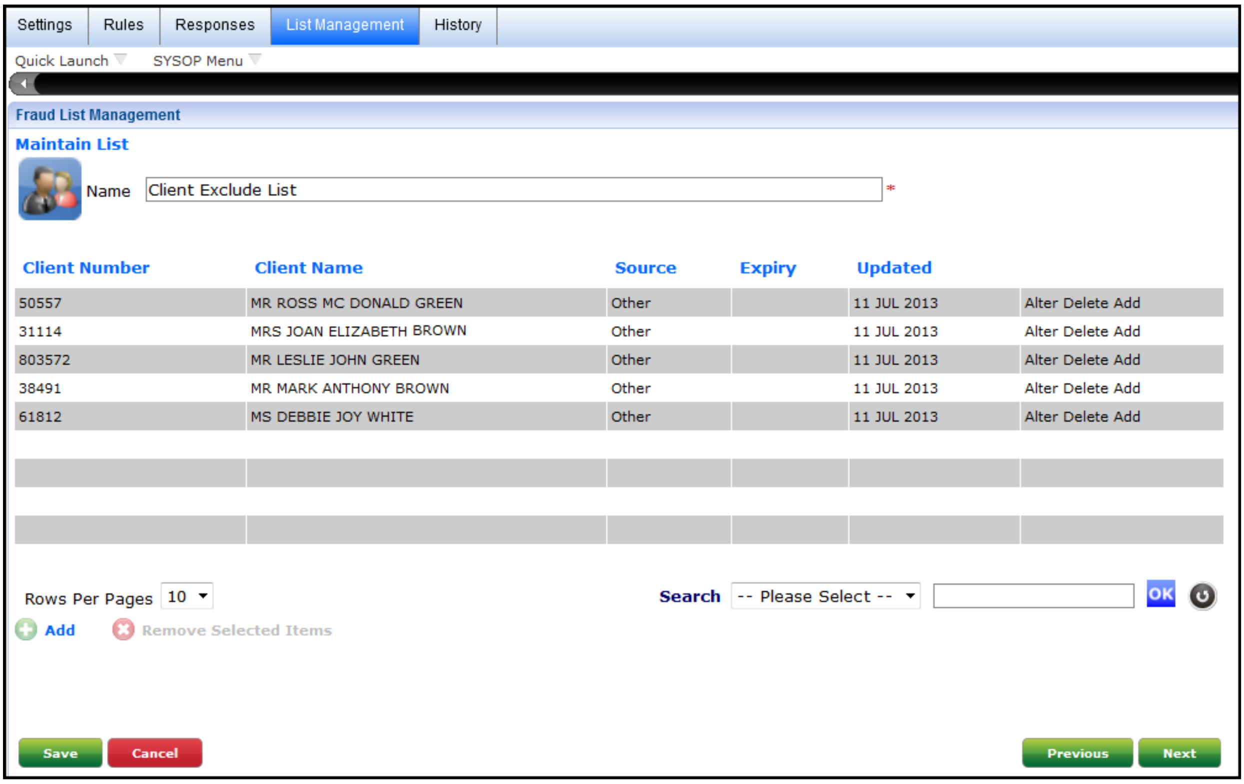
Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	Select the MCC List you created for this rule from the 'Lists to Include in monitoring' drop-down list. 'Lists to Exclude from monitoring' should be left as "-- Please Select --". A client list (Include or Exclude) is optional and if both are left unselected, all clients will be included in this rule.
Transaction Amount	This rule is to be triggered by a single transaction of more than $500 so '500.01' is entered into this field.

Transaction Codes	Select the appropriate transaction codes relating to the type of transaction likely (e.g. VISA Cash Advance, VISA Retail Purchase). You may also select other transactions if you consider them appropriate, e.g. ATM/POS Withdrawal if this rule is to cover VISA Debit Cards using the 'debit' mode on a POS terminal.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By setting this field to 'All' you can capture Internet gambling (i.e. card not present) transactions as well.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

Any foreign VISA transaction greater than $10,000

This rule is triggered by any foreign VISA transaction more than $10,000. As this is only for foreign transactions, select all countries other than your own.

Fraud List Management



Maintain List

Name: Client Exclude List *

Client Number	Client Name	Source	Expiry	Updated	
50557	MR ROSS MC DONALD GREEN	Other		11 JUL 2013	Alter Delete Add
31114	MRS JOAN ELIZABETH BROWN	Other		11 JUL 2013	Alter Delete Add
803572	MR LESLIE JOHN GREEN	Other		11 JUL 2013	Alter Delete Add
38491	MR MARK ANTHONY BROWN	Other		11 JUL 2013	Alter Delete Add
61812	MS DEBBIE JOY WHITE	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages: 10

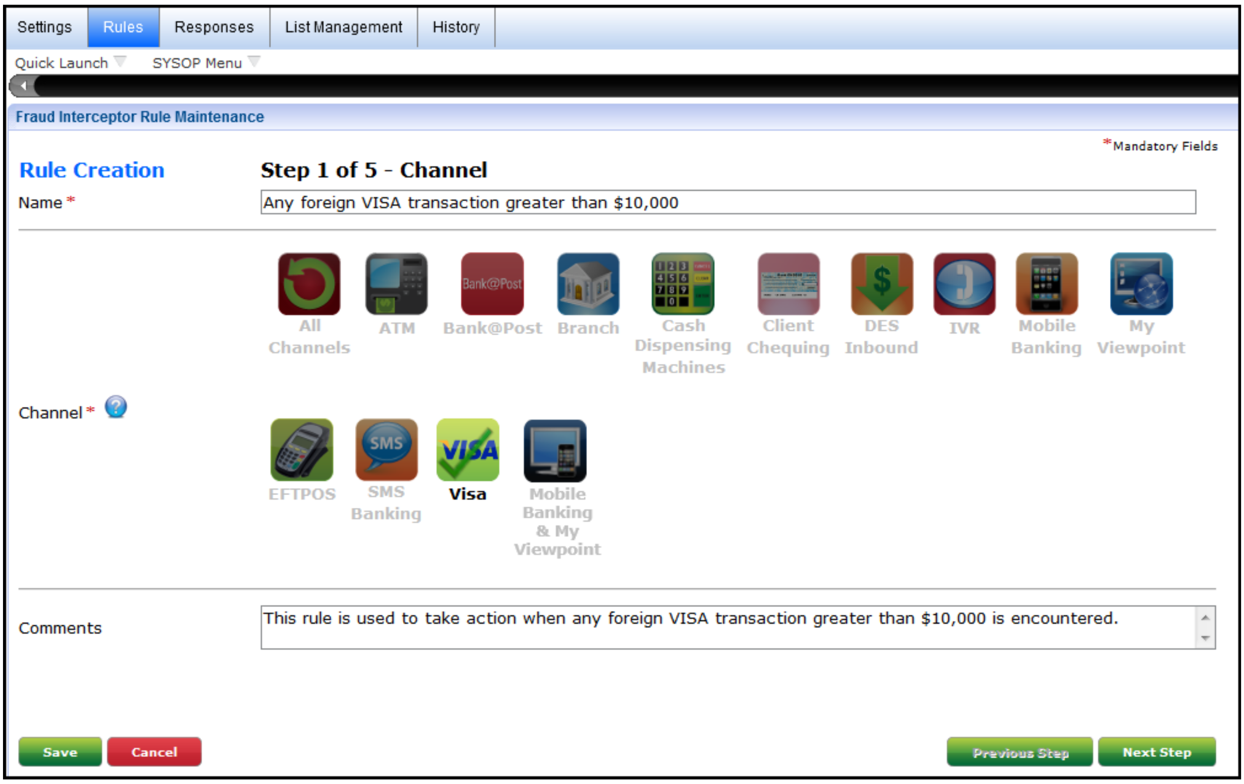
Search: -- Please Select --

Add

Remove Selected Items

The Client Exclude List contains the details of clients who will not be included in this rule. You can use this List to cater for known low-risk clients who you would expect to trigger this rule on recurring basis.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

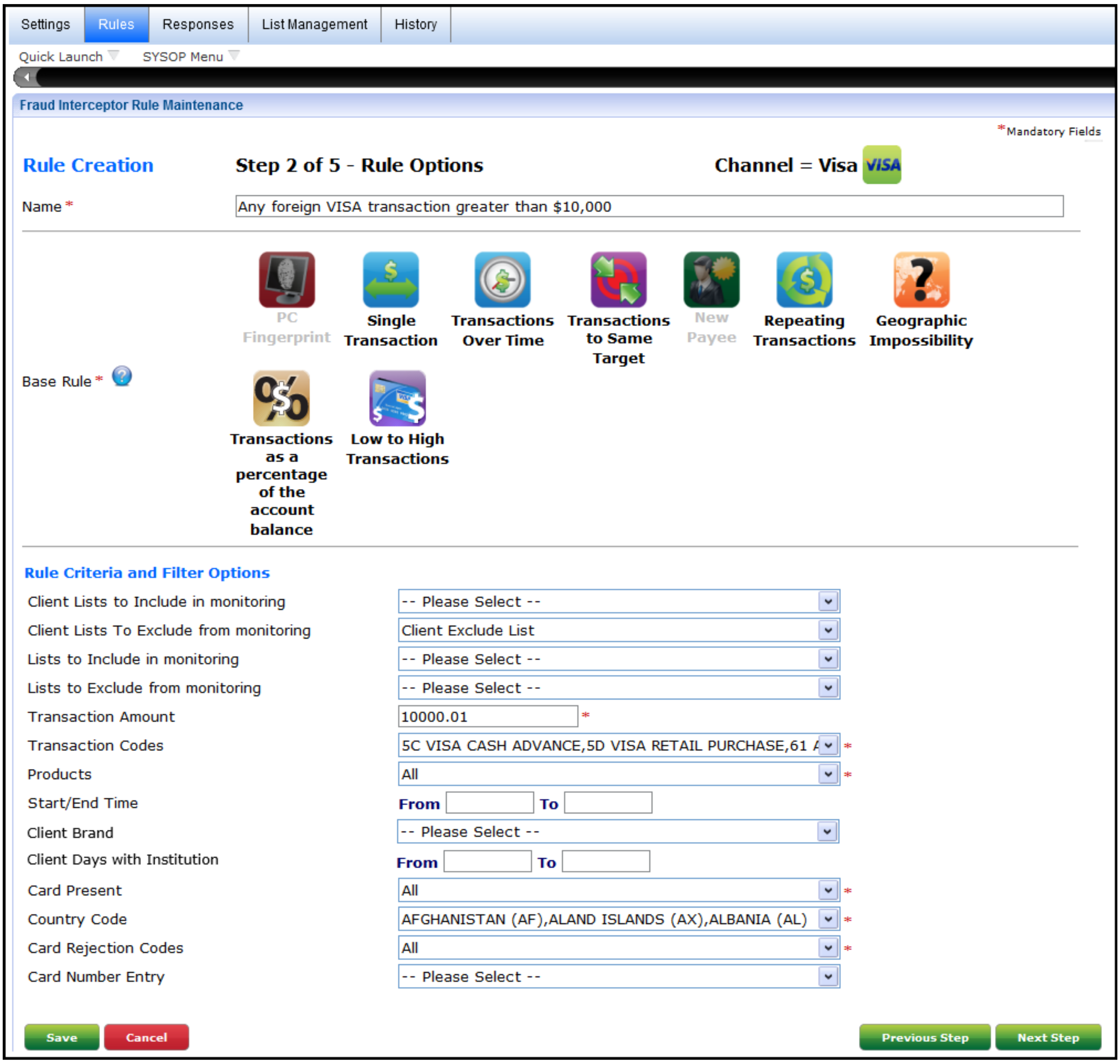
Name *: Any foreign VISA transaction greater than $10,000

Channel *: Visa

Comments: This rule is used to take action when any foreign VISA transaction greater than $10,000 is encountered.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation **Step 2 of 5 - Rule Options** **Channel = Visa** VISA

Name * Any foreign VISA transaction greater than $10,000

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Client Exclude List
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	10000.01 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE,61 A *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	AFGHANISTAN (AF),ALAND ISLANDS (AX),ALBANIA (AL) *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Single Transaction'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	You can optionally exclude known 'safe' clients. This has been done by selecting the "Client Exclude List" from the 'Client Lists to Exclude from Monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --".
Transaction Amount	This rule is to be triggered by a single transaction of more than $10000 so '10000.01' is entered into this field.

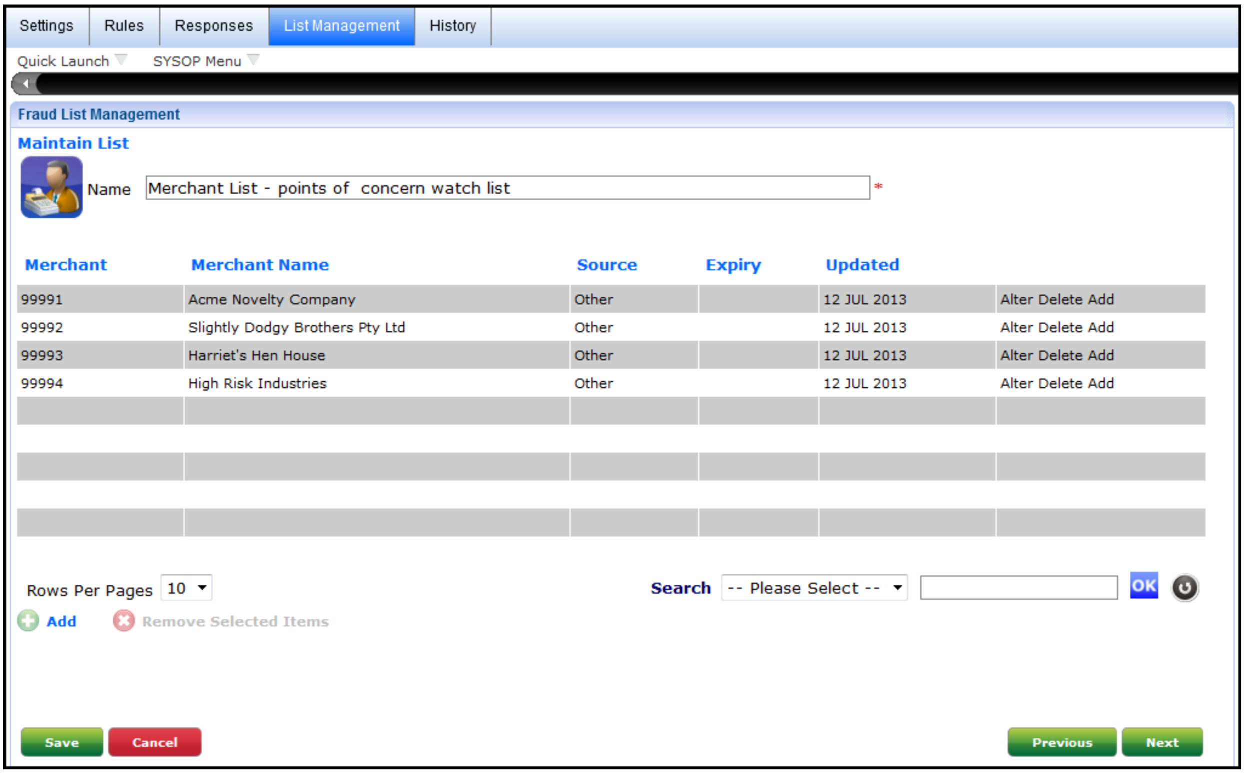
Transaction Codes	This rule only applies to VISA debit transactions and may include ATM transactions. Select the appropriate transaction codes from the drop-down list.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	This field must be set to 'All' which will allow the capture of merchant transactions, ATM transactions and Internet or phone transactions.
Country Code	Select all countries other than your own. The easiest way to do this is to select the 'All' option from the drop-down list and then deselect your own country.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

Any transaction from specific merchants identified as points of concern

This rule will be triggered by matching transactions to a list made using the Merchant Names List option. The list needs to be created before you create the rule.

This rule relates to the VISA channel. You may have been provided with a list of Merchant IDs for potentially suspect VISA transactions; however, the merchant name rule matching is performed on the merchant name and not on the Merchant ID or number. Note that matches to merchant names are not case sensitive.

Fraud List Management



Name: Merchant List - points of concern watch list *

Merchant	Merchant Name	Source	Expiry	Updated	
99991	Acme Novelty Company	Other		12 JUL 2013	Alter Delete Add
99992	Slightly Dodgy Brothers Pty Ltd	Other		12 JUL 2013	Alter Delete Add
99993	Harriet's Hen House	Other		12 JUL 2013	Alter Delete Add
99994	High Risk Industries	Other		12 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

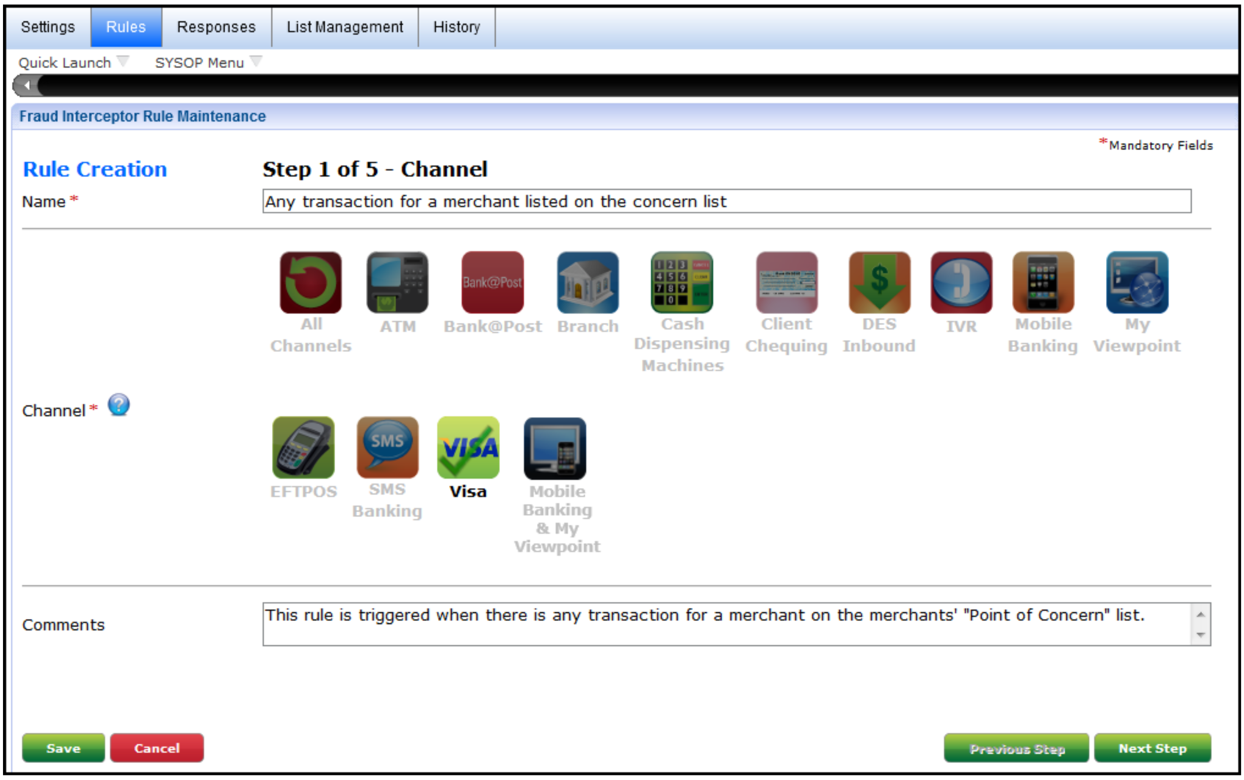
In setting up the merchant Lists, the operator may choose to use “wildcards” with the merchant name. This means that a single instance of a merchant name parameter can be used to test the incoming transaction for a variety of pattern matches.

For example, if the merchant name is entered as *SHONKY* (with the asterisks being the wildcard characters), then any transaction with the merchant name found to *include* the character string “SHONKY” will match the List criteria.

Likewise, if the merchant name parameter were entered as SHONKY*, any transaction where the merchant name begins with “SHONKY” will meet the criteria. If entered as *SHONKY, the merchant name match will occur when the name ends with “SHONKY”.

Wildcards can also be used as delimiters. For example, you can enter NIGERIAN*BANK*. Merchant names meeting this criterion would include “NIGERIAN CENTRAL BANK”, “NIGERIAN BANK LTD”, “NIGERIAN PETROLEUM BANKING CORPORATION” etc. A merchant named “CENTRAL NIGERIAN BANK” would not match as the parameter indicates that the string has to start with NIGERIAN and include the word BANK. In order for the parameter to cover such a merchant name, the parameter could simply be set to be *NIGERIAN*BANK*.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

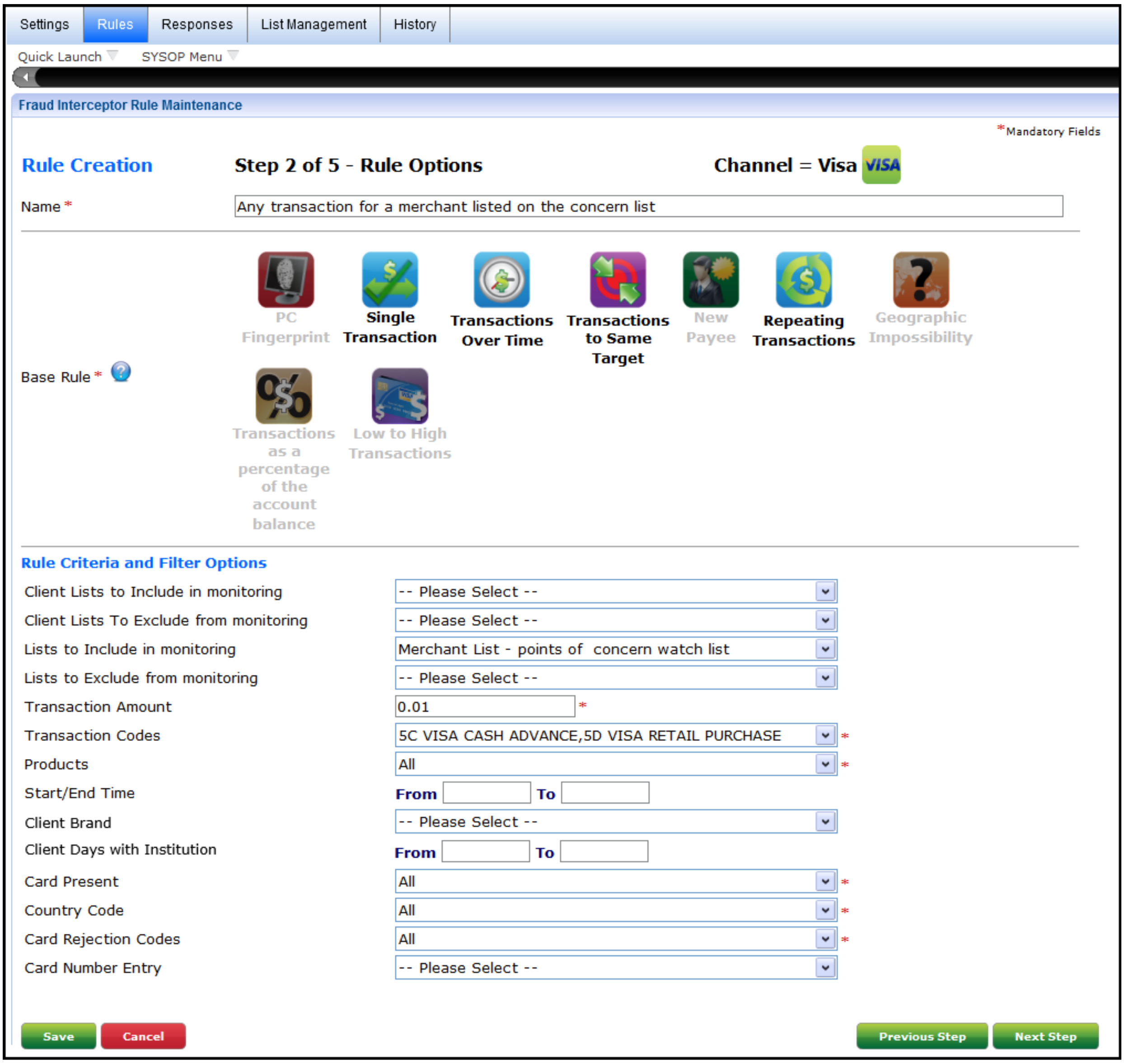
Name *: Any transaction for a merchant listed on the concern list

Channel *: Visa

Comments: This rule is triggered when there is any transaction for a merchant on the merchants' "Point of Concern" list.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation — Step 2 of 5 - Rule Options — Channel = Visa

Name * Any transaction for a merchant listed on the concern list

Base Rule * Single Transaction

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Merchant List - points of concern watch list
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	0.01 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Single Transaction'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	The merchant list you created previously is picked up from the 'Lists to Include in monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --" although you could use a client exclude or include list if required.
Transaction Amount	This rule is to be triggered for any transaction from the merchants in your list. A nominal value of 0.01 should be entered into this field.
Transaction Codes	This rule only applies to VISA debit transactions. Select VISA Cash Advance and VISA Retail Purchase from the list of transaction cards.

Products	'All' has been selected; however, if you only have one or two product types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	This field should be set to 'All' to capture both card present and card not present transactions.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

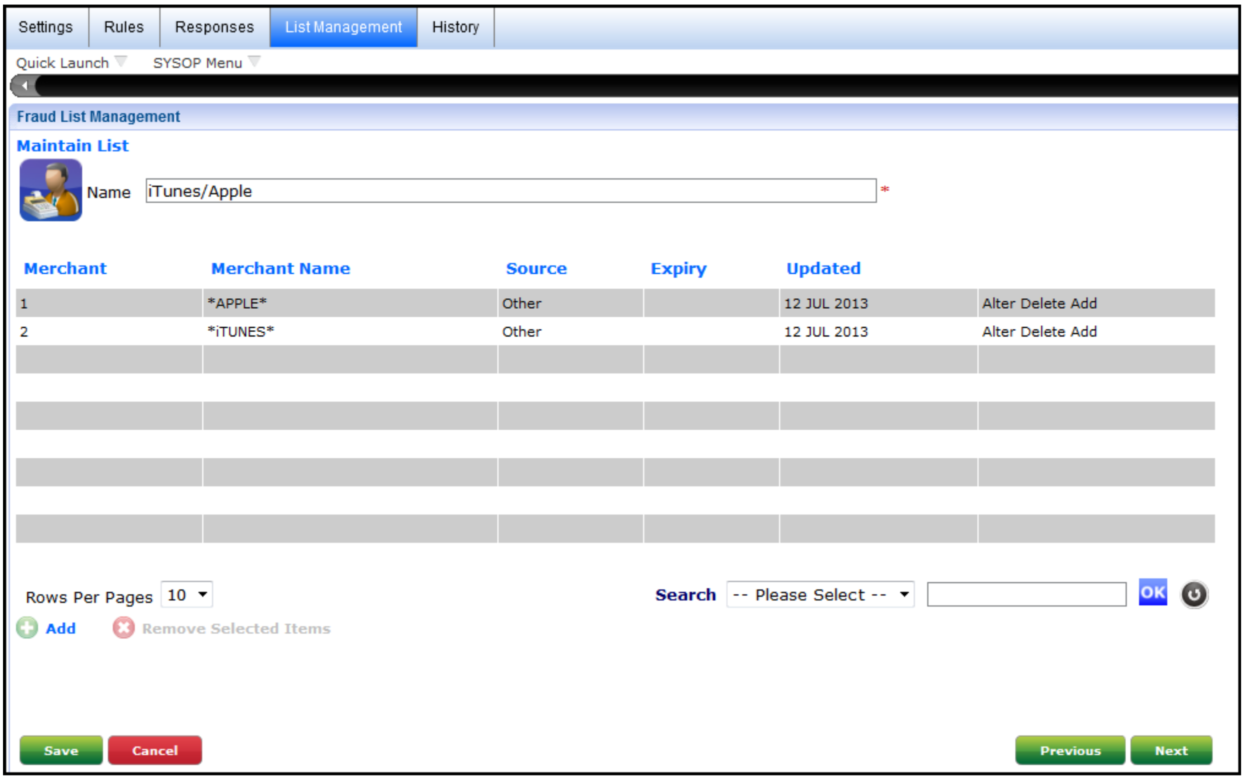
VISA - iTunes/Apple, overseas transactions

This rule is triggered when there are two or more VISA transactions within a 24 hour period from iTunes or Apple from an overseas country. Matching is based on the merchant name and is primarily aimed at detecting transactions related to purchases via iTunes or the Apple App Store that originate from overseas.

Before creating this rule, you will need to create a Merchants type Fraud List capture only merchants names that include iTunes or Apple.

If you have clients who regularly make overseas purchases from iTunes or Apple, you can also create a client exclusion list to prevent these clients from being captured by the rule.

Fraud List Management



Name: iTunes/Apple *

Merchant	Merchant Name	Source	Expiry	Updated	
1	*APPLE*	Other		12 JUL 2013	Alter Delete Add
2	*iTUNES*	Other		12 JUL 2013	Alter Delete Add

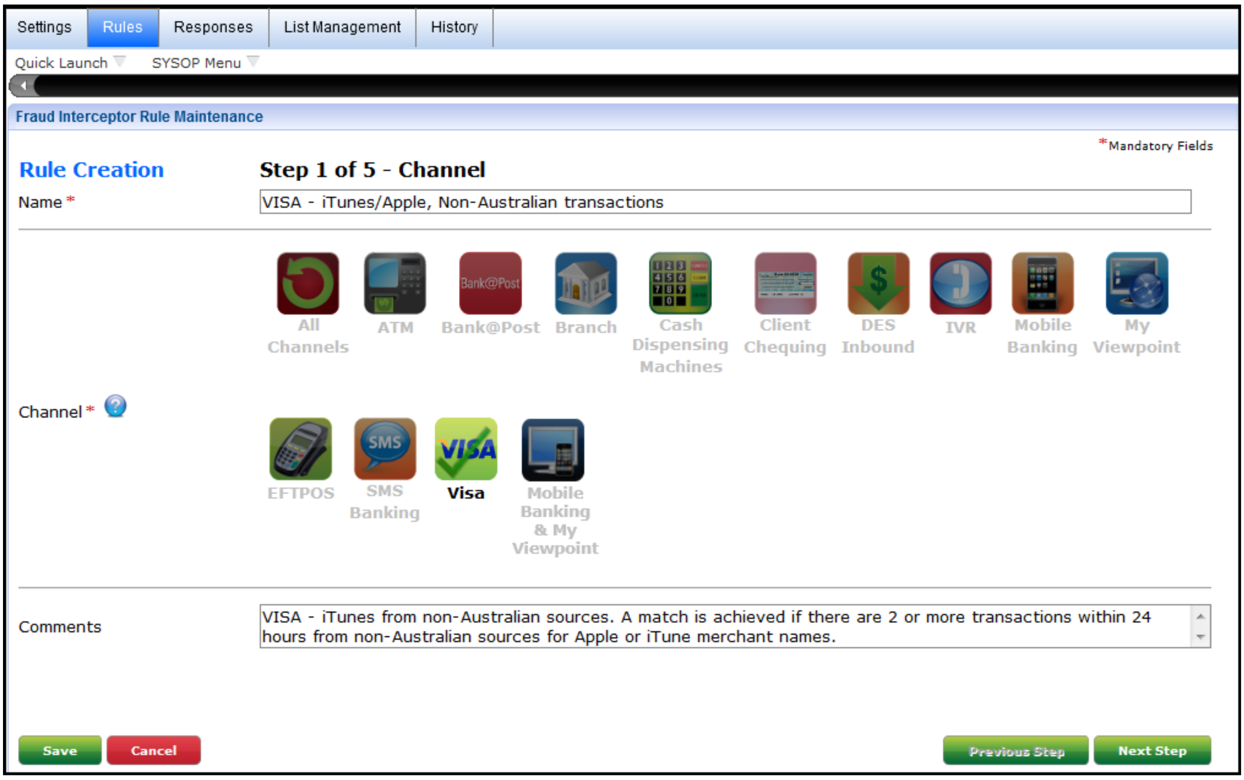
Rows Per Pages: 10

Search: -- Please Select --

The iTunes/Apple list contains the merchant name search strings to include in this rule. For simplicity, wild cards have been used to ensure matches to all variations of Apple and iTunes. Note that matches to merchant names are not case sensitive.

If you find that this results in too many false matches, you can use variations on these names.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Step 1 of 5 - Channel

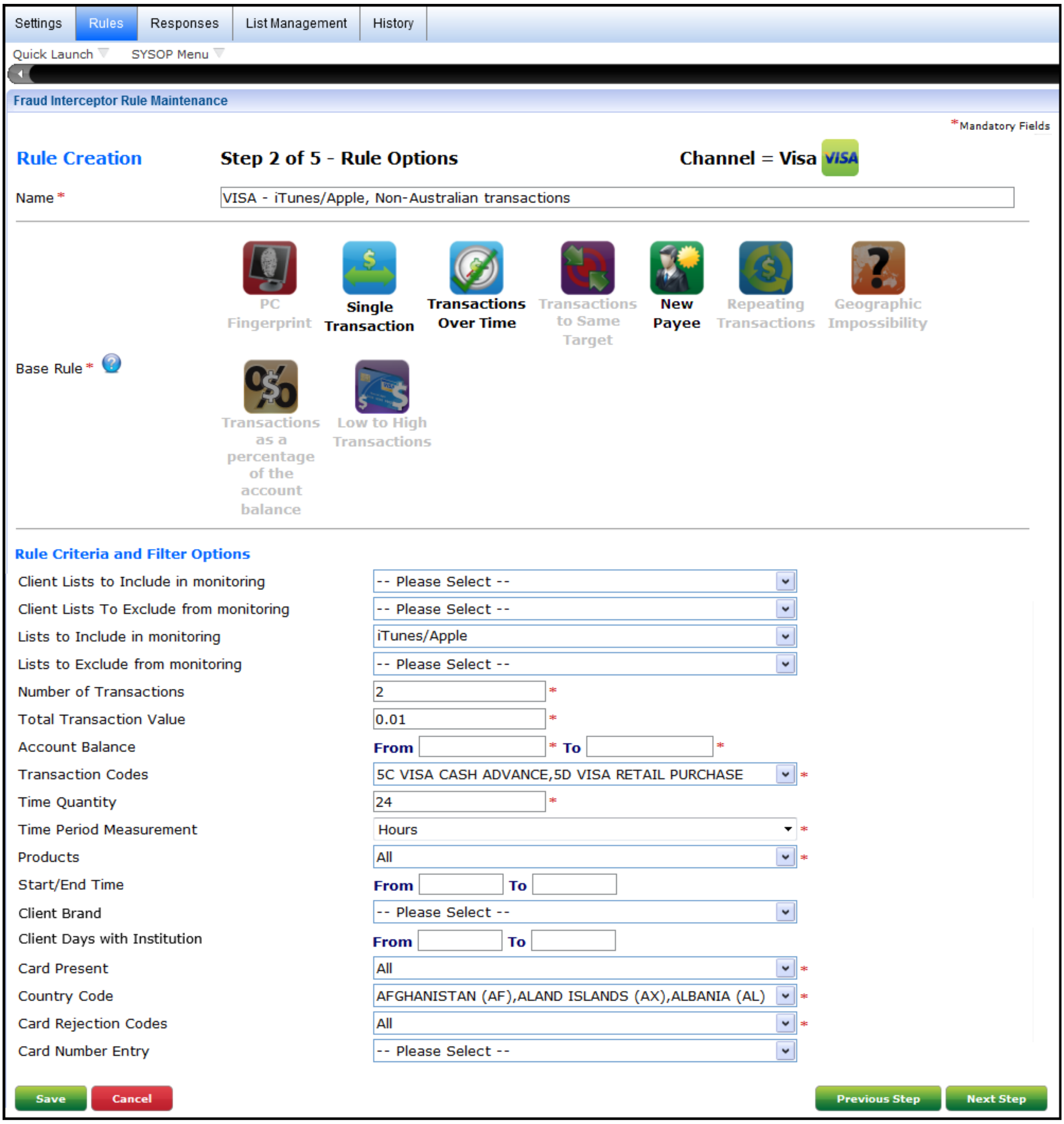
Name *: VISA - iTunes/Apple, Non-Australian transactions

Channel *: Visa

Comments: VISA - iTunes from non-Australian sources. A match is achieved if there are 2 or more transactions within 24 hours from non-Australian sources for Apple or iTune merchant names.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Visa**

Name * VISA - iTunes/Apple, Non-Australian transactions

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	iTunes/Apple
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	2 *
Total Transaction Value	0.01 *
Account Balance	From * To *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	AFGHANISTAN (AF),ALAND ISLANDS (AX),ALBANIA (AL) *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	The Merchants List you created for this rule has been selected from the drop-down list 'Lists to Include in monitoring'. A client list (Include or Exclude) is optional; if both Include and Exclude lists are left unselected, all clients will be included in this rule. 'Lists to Exclude from monitoring' should be left as "-- Please Select --".

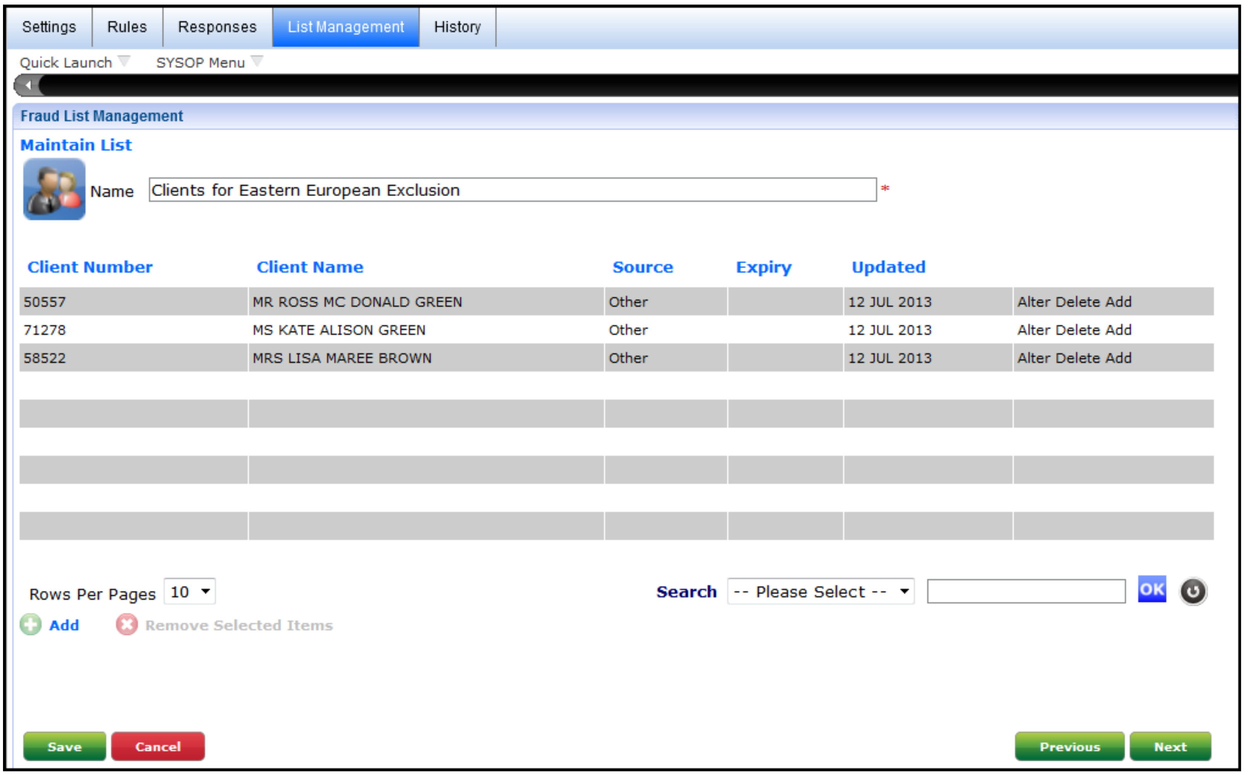
Number of Transactions	If you enter '2' into this field, there must be at least two transactions within the specified time period.
Total Transaction Value	As this rule is to apply when there are two or more transactions, the total transaction value can be entered as a nominal amount, e.g. 0.01.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. The minimum you are likely to require are VISA Cash Advance and VISA Retail Purchase codes. You may also include other codes, if you consider those codes appropriate.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected, however, you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By selecting 'All' you are catering for personal transactions as well as telephone and Internet transactions.
Country Code	Select all countries other than your own. The easiest way to do this is to select the 'All' option from the drop-down list and then deselect your own country.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

VISA - Any transactions to selected Russian/Eastern European countries

This rule is triggered when a VISA transaction originates from selected Russian or Eastern European countries. A client exclusion list has been created to prevent clients who regularly transact with the countries covered by this rule from being captured. The use of such an exclusion list is optional.

Fraud List Management

The Clients for Eastern European Exclusion list contains the list of all clients who are known to be low risk and regularly transact with countries captured by this rule.



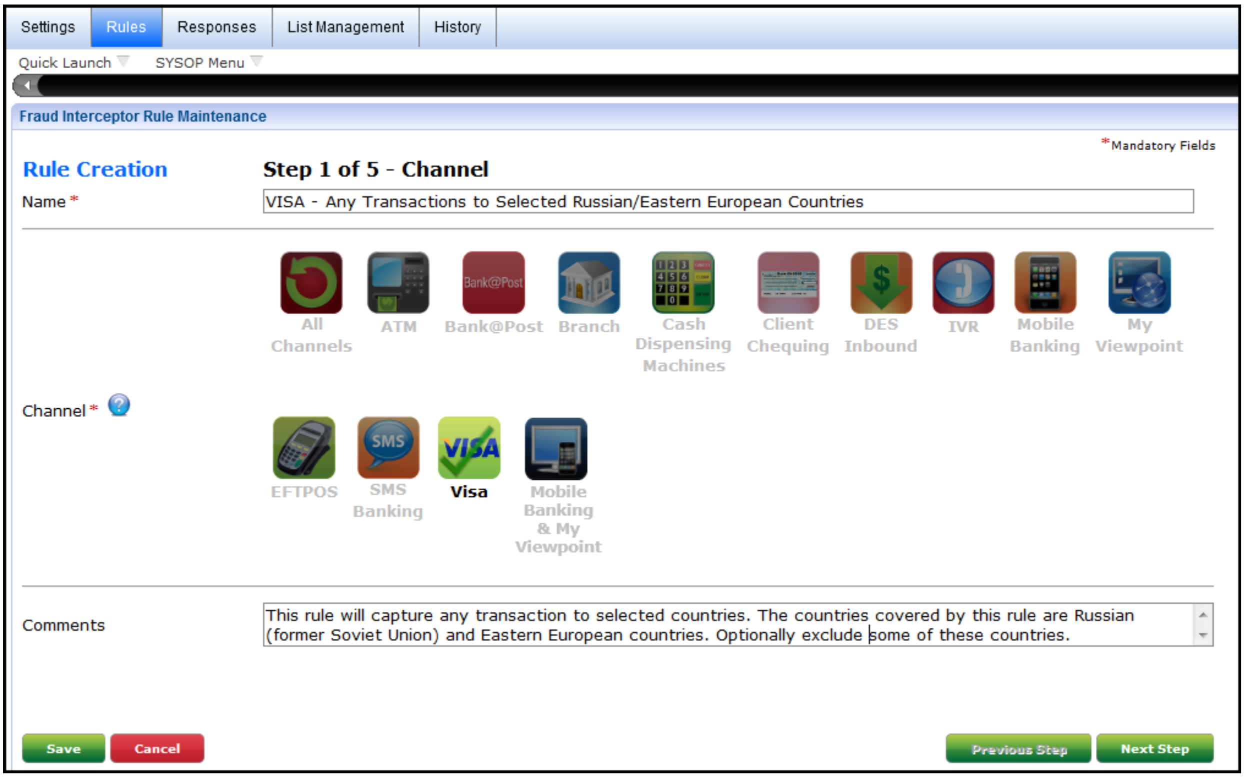
Name: Clients for Eastern European Exclusion *

Client Number	Client Name	Source	Expiry	Updated	
50557	MR ROSS MC DONALD GREEN	Other		12 JUL 2013	Alter Delete Add
71278	MS KATE ALISON GREEN	Other		12 JUL 2013	Alter Delete Add
58522	MRS LISA MAREE BROWN	Other		12 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Rule Creation

Step 1 of 5 - Channel

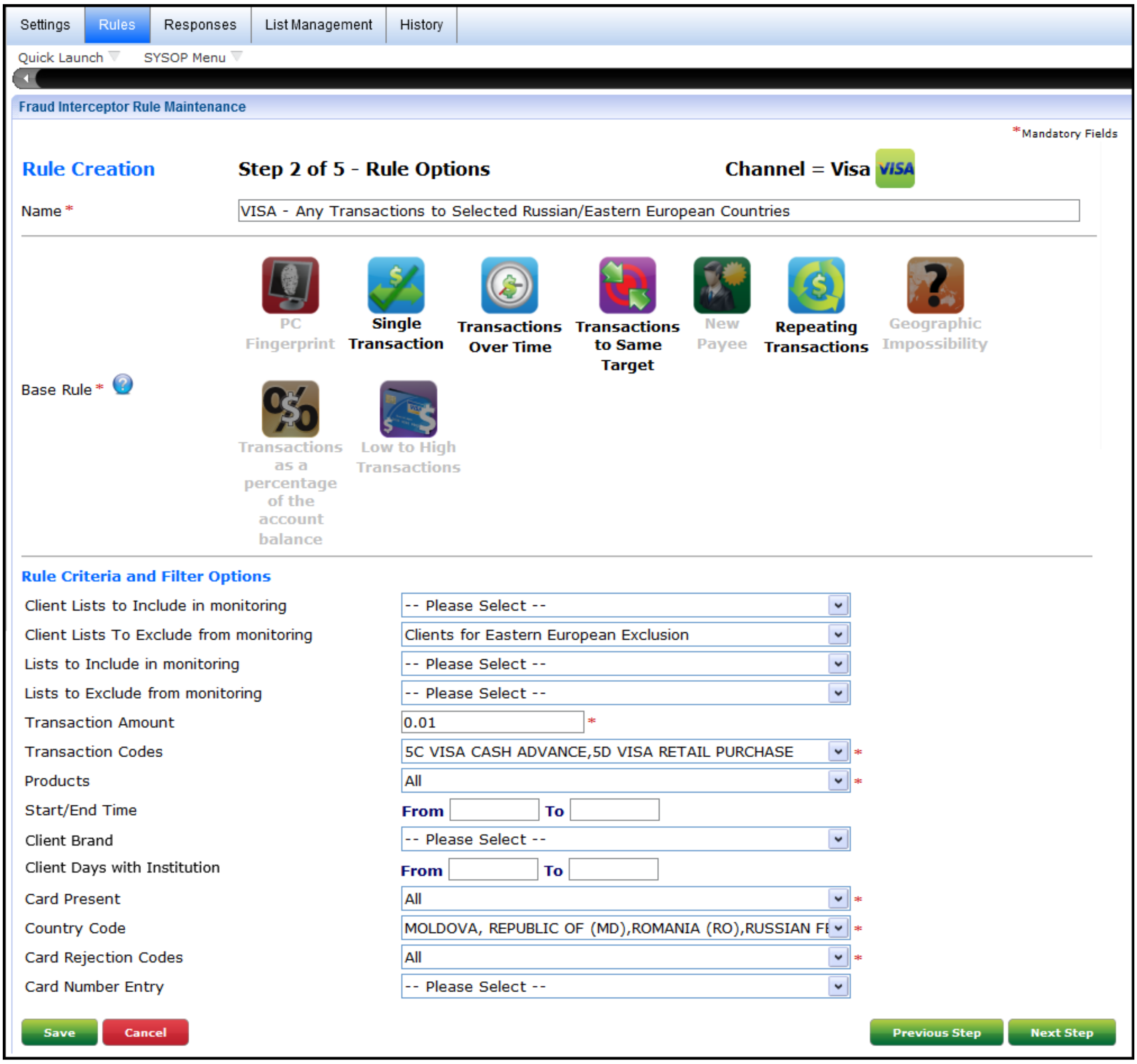
Name * VISA - Any Transactions to Selected Russian/Eastern European Countries

Channel *

Comments This rule will capture any transaction to selected countries. The countries covered by this rule are Russian (former Soviet Union) and Eastern European countries. Optionally exclude some of these countries.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Name * VISA - Any Transactions to Selected Russian/Eastern European Countries

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Clients for Eastern European Exclusion
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	0.01 *
Transaction Codes	5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	MOLDOVA, REPUBLIC OF (MD),ROMANIA (RO),RUSSIAN FE *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Single Transaction'.

The following criteria and filter options have been specified:

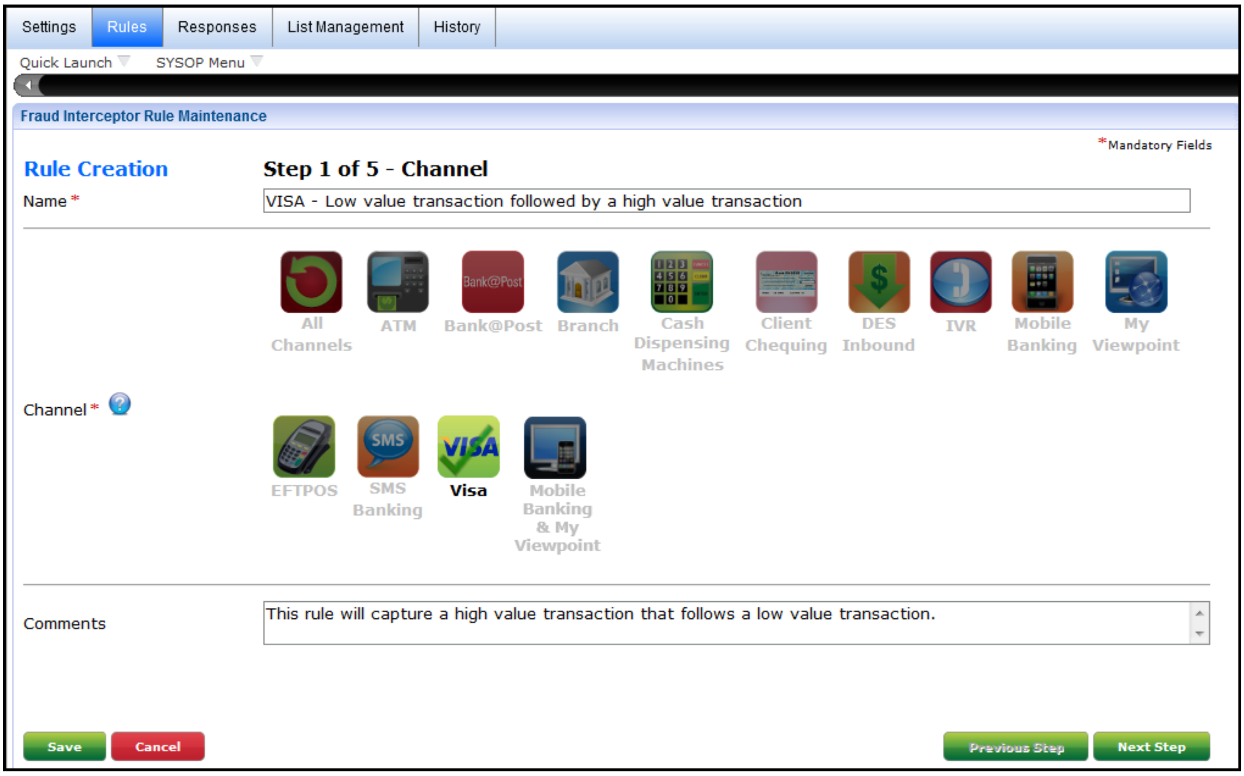
Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	You can optionally exclude known 'safe' clients. This has been done by selecting the "Clients for Eastern European Exclusion" list from the 'Client Lists to Exclude from Monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --".
Transaction Amount	This rule is to be triggered by a single transaction. The value of the transaction should be low so a nominal value of 0.01 will be sufficient.

Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. The minimum you are likely to require are VISA Cash Advance and VISA Retail Purchase codes. You may also include other codes such as ATM/POS Withdrawal, if you consider those codes appropriate.
Products	'All' has been selected, however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By selecting 'All' you are catering for personal transactions as well as telephone and Internet transactions.
Country Code	Select the countries you require from the drop-down list.
Card Rejection Codes	In this example, 'All' has been selected to include failed transaction attempts.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example.

VISA - Low value transaction followed by a high value transaction

This rule looks at two transactions within a given time period. If a low value transaction is followed by a high value transaction within the time period provided, this rule will be triggered.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Rule Creation — **Step 1 of 5 - Channel**

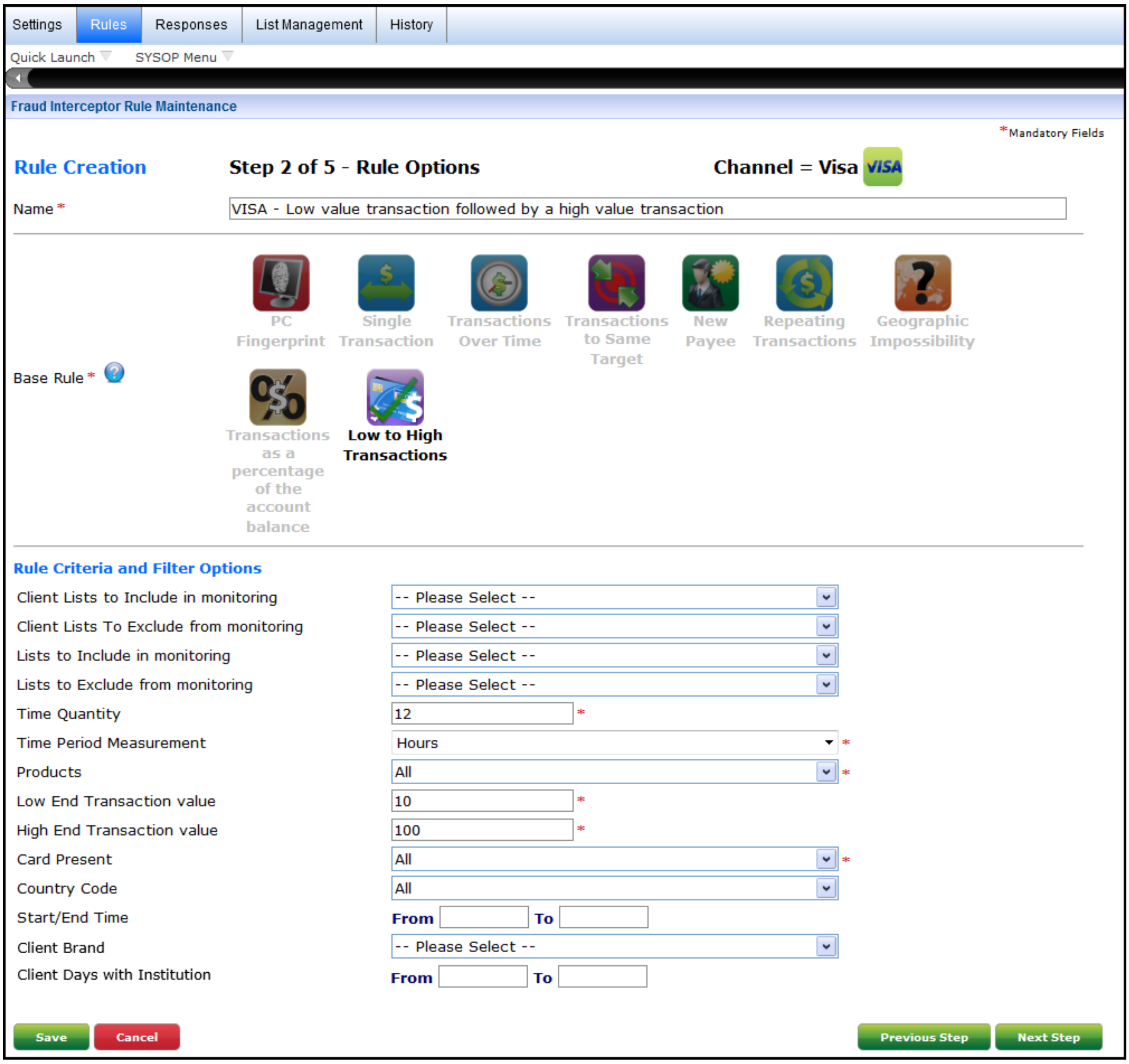
Name *: VISA - Low value transaction followed by a high value transaction

Channel *: Visa

Comments: This rule will capture a high value transaction that follows a low value transaction.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation Step 2 of 5 - Rule Options Channel = Visa

Name * VISA - Low value transaction followed by a high value transaction

Base Rule * Low to High Transactions

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Time Quantity	12 *
Time Period Measurement	Hours *
Products	All *
Low End Transaction value	10 *
High End Transaction value	100 *
Card Present	All *
Country Code	All
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To

This rule uses the Base Rule 'Low to High Transactions'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	There are no lists selected in this example; however, you could use client and other lists to suit your needs; for example, you could use a client list to exclude clients you know are low risk and frequently have a transaction pattern that would falsely trigger this rule.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '12' and 'Hours' have been selected. This is the maximum time period between the low value transaction and the high value transaction which will be considered for triggering this rule.

Products	'All' has been selected, however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Low End Transaction Value	This is the maximum value of the low value transaction which will be used to trigger a match with this rule. You can enter a value of up to two decimal places.
High End Transaction Value	Transaction values above the amount entered into this field will be used to trigger a match with this rule. You can enter a value of up to two decimal places.
Card Present	By setting this field to 'All' to capture both card present and card not present transactions.
Country Code	By selecting 'All' every country is included.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.

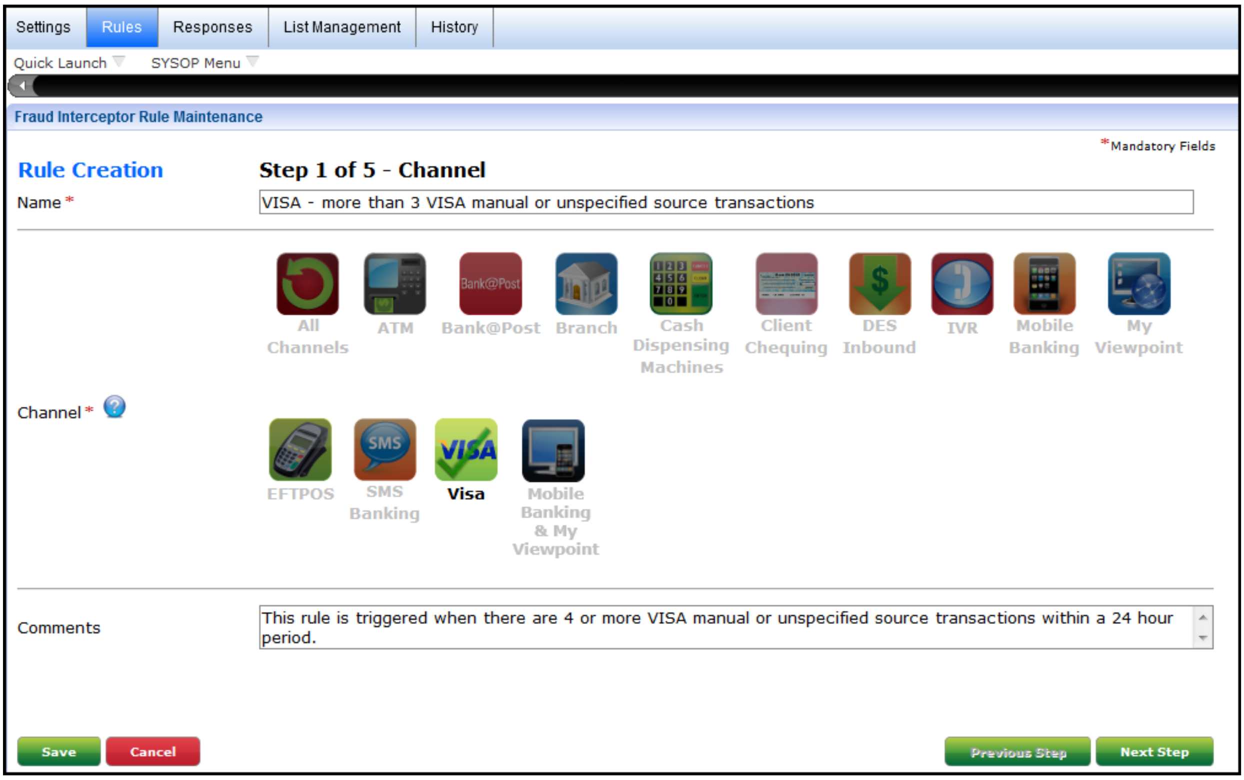
VISA - More than three VISA manual or unspecified source transactions (Card Number Entry)

Functionality is included in most VISA channel Base Rules to consider the method by which the card number is acquired. The Base Rules which may include the card number are:

- Single Transaction
- Transactions Over Time
- Transactions to Same Target
- Repeating Transactions
- Transactions as a Percentage of Balance.

This rule is considering manual and unspecified source transactions. The rule is triggered if there are more than three manual or unspecified source transactions within a 24 hour period. Transactions that add to more than $100 will be included in the rule.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Step 1 of 5 - Channel

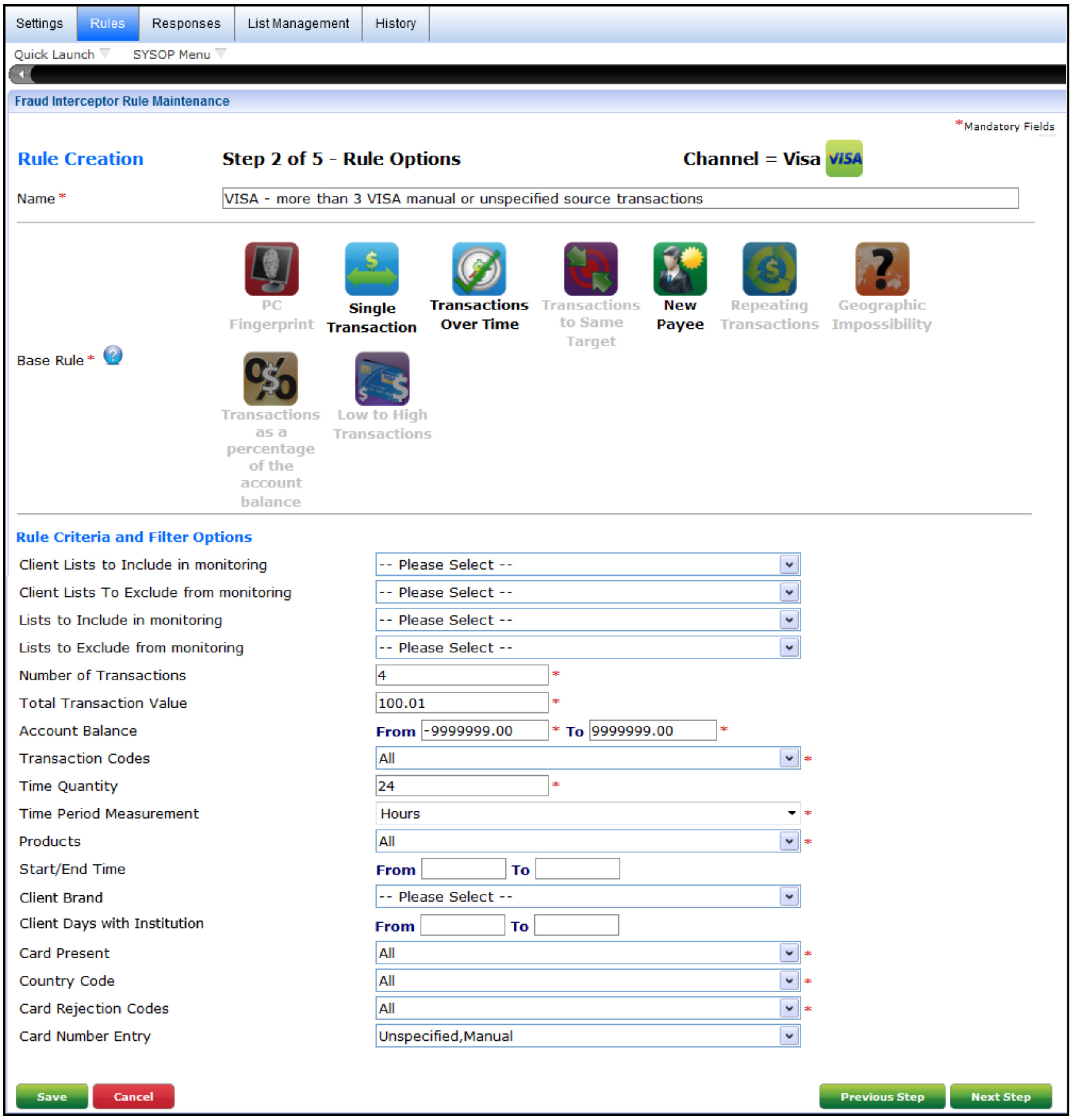
Name *: VISA - more than 3 VISA manual or unspecified source transactions

Channel *: Visa

Comments: This rule is triggered when there are 4 or more VISA manual or unspecified source transactions within a 24 hour period.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation — **Step 2 of 5 - Rule Options** — **Channel = Visa**

Name * VISA - more than 3 VISA manual or unspecified source transactions

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	4 *
Total Transaction Value	100.01 *
Account Balance	From -9999999.00 * To 9999999.00 *
Transaction Codes	All *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	Unspecified,Manual

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	There are no lists selected in this example; however, you could use client and other lists to suit your needs; for example, you could use a client list to exclude clients you know are low risk and frequently have a transaction pattern that would falsely trigger this rule.
Number of Transactions	If you enter '4' into this field, there must be at least four transactions within the specified time period.

Total Transaction Value	As this rule is to apply to the sum of transactions over $100 and the field itself will include the value entered, you need to enter 100.01 (or 101 if you are not concerned with cents).
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list or select 'All'. The minimum you are likely to require are VISA Cash Advance and VISA Retail Purchase codes. You may also include other codes, such as ATM/POS Withdrawal, if you consider those codes appropriate.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected, however you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule to enable the rule to operate 24 hours a day.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	By selecting 'All' you are catering for personal transactions as well as telephone and Internet transactions.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	Select 'All' for every card rejection code, or select one or more individual codes. Only the selected code values will be examined with this rule. In this example, 'All' has been selected to include failed transaction attempts.

<table>
<tr>
<td><b>Card Number Entry</b></td>
<td>
<p>The method by which the card number is acquired. This allows you to differentiate rules based upon how the card transaction was initiated, for example a rule could be set up to monitor only PayWave transactions. Likewise, a rule could be setup to monitor all transactions except chip initiated.</p>
<p>If the Card Present option is used, this will negate selections in Card Number Entry that conflict. For example, if the Card Present is set to "No" and the Card Number Entry is set to "Chip" the rule will not find any transactions as no Chip initiated transactions are Card Not Present. The below table shows the relationship between Card Number Entry and Card Present.</p>
<table>
<tr><th>Card Number Entry</th><th>Card Present</th></tr>
<tr><td>Not Specified</td><td>No</td></tr>
<tr><td>Manual</td><td>No</td></tr>
<tr><td>Magnetic Stripe</td><td>Yes</td></tr>
<tr><td>Barcode</td><td>No</td></tr>
<tr><td>OCR</td><td>No</td></tr>
<tr><td>Chip</td><td>Yes</td></tr>
<tr><td>Contactless - Card/Pay/Way</td><td>Yes</td></tr>
<tr><td>Contactless - Manual Entry</td><td>No</td></tr>
<tr><td>Contactless - Magnetic Strip</td><td>Yes</td></tr>
<tr><td>eftpos Card Not Present</td><td>No</td></tr>
<tr><td>Magnetic Stripe Fallback</td><td>Yes</td></tr>
</table>
</td>
</tr>
</table>

VISA - Card rejection codes

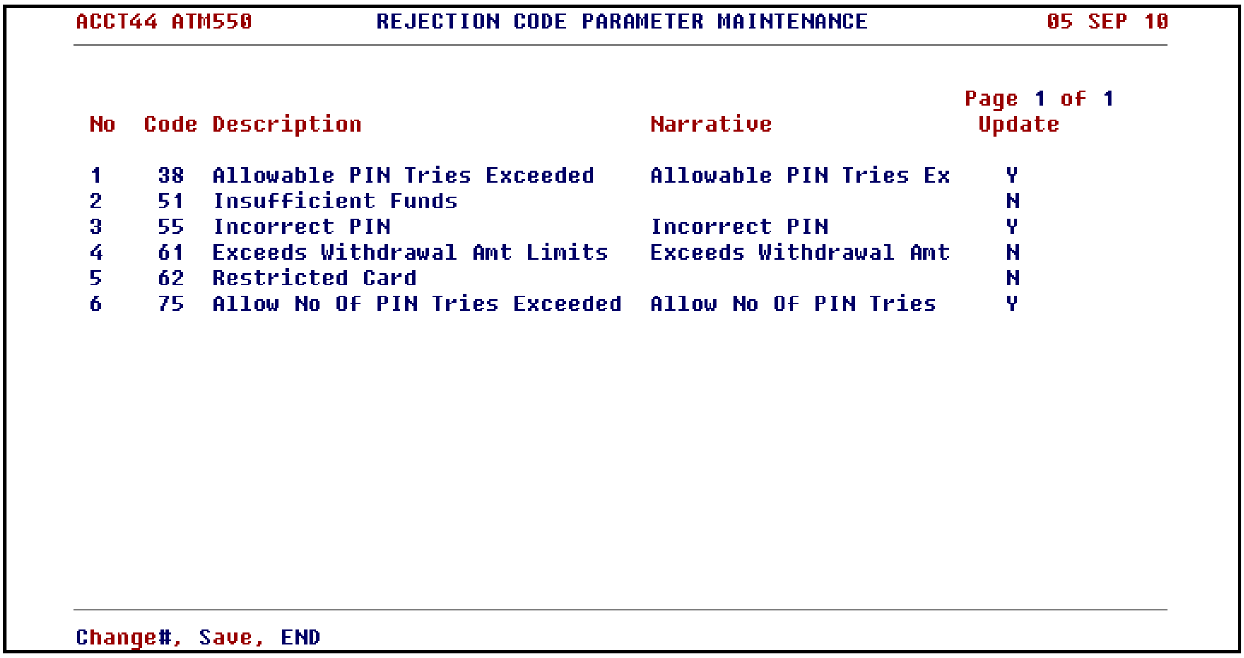
VISA transactions can be declined for a number of reasons, for example, insufficient funds, incorrect account selection and incorrect PINs (Personal Identification Numbers).

This rule looks at multiple declined transactions. The declines may be due to insufficient funds, account selection, incorrect PINs and other factors. This rule differs from other declined transaction functionality in that it looks at the actual decline actions built into the credit card system rather than looking for transactions that are declined after a match to fraud rule.

This rule works by looking at declined transaction codes as listed on the **Rejection Code Parameter Maintenance** page. These rejection codes may be used for ATM, VISA, POS and Bank@Post channels.

In this example, the rule will be triggered for the following card rejection codes:

- Allowable PIN Tries Exceeded (38)
- Incorrect PIN (55)
- Allow No Of PIN Tries Exceeded (75).

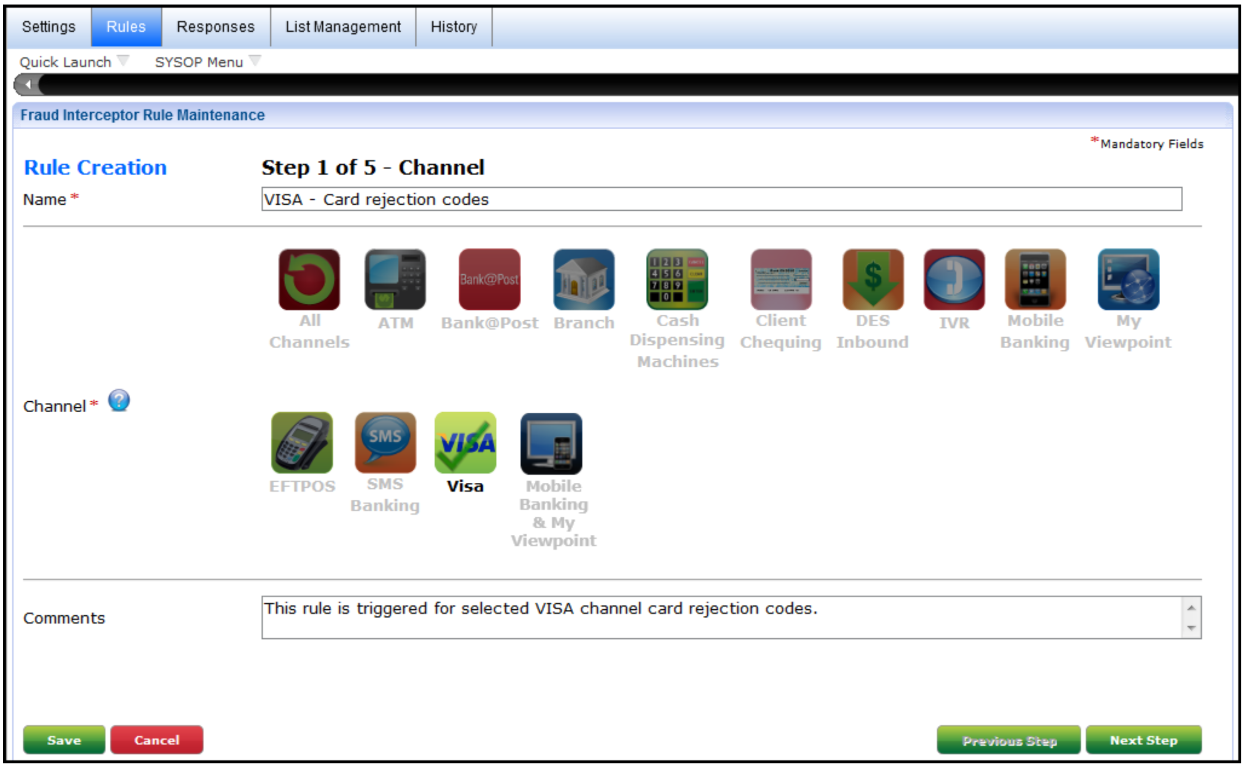


```
ACCT44 ATM550          REJECTION CODE PARAMETER MAINTENANCE            05 SEP 10


                                                                Page  1 of  1
 No   Code Description                     Narrative               Update

 1     38  Allowable PIN Tries Exceeded    Allowable PIN Tries Ex     Y
 2     51  Insufficient Funds                                         N
 3     55  Incorrect PIN                   Incorrect PIN              Y
 4     61  Exceeds Withdrawal Amt Limits   Exceeds Withdrawal Amt     N
 5     62  Restricted Card                                            N
 6     75  Allow No Of PIN Tries Exceeded  Allow No Of PIN Tries      Y










Change#, Save, END
```

In order for this rule to work, a non-transaction narrative must be generated. In order to generate the transaction narrative to the client's account, ensure Update" is set to "Y"es.

The rule will be triggered when there are at least 3 transactions with these rejection codes within any 24 hour period.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



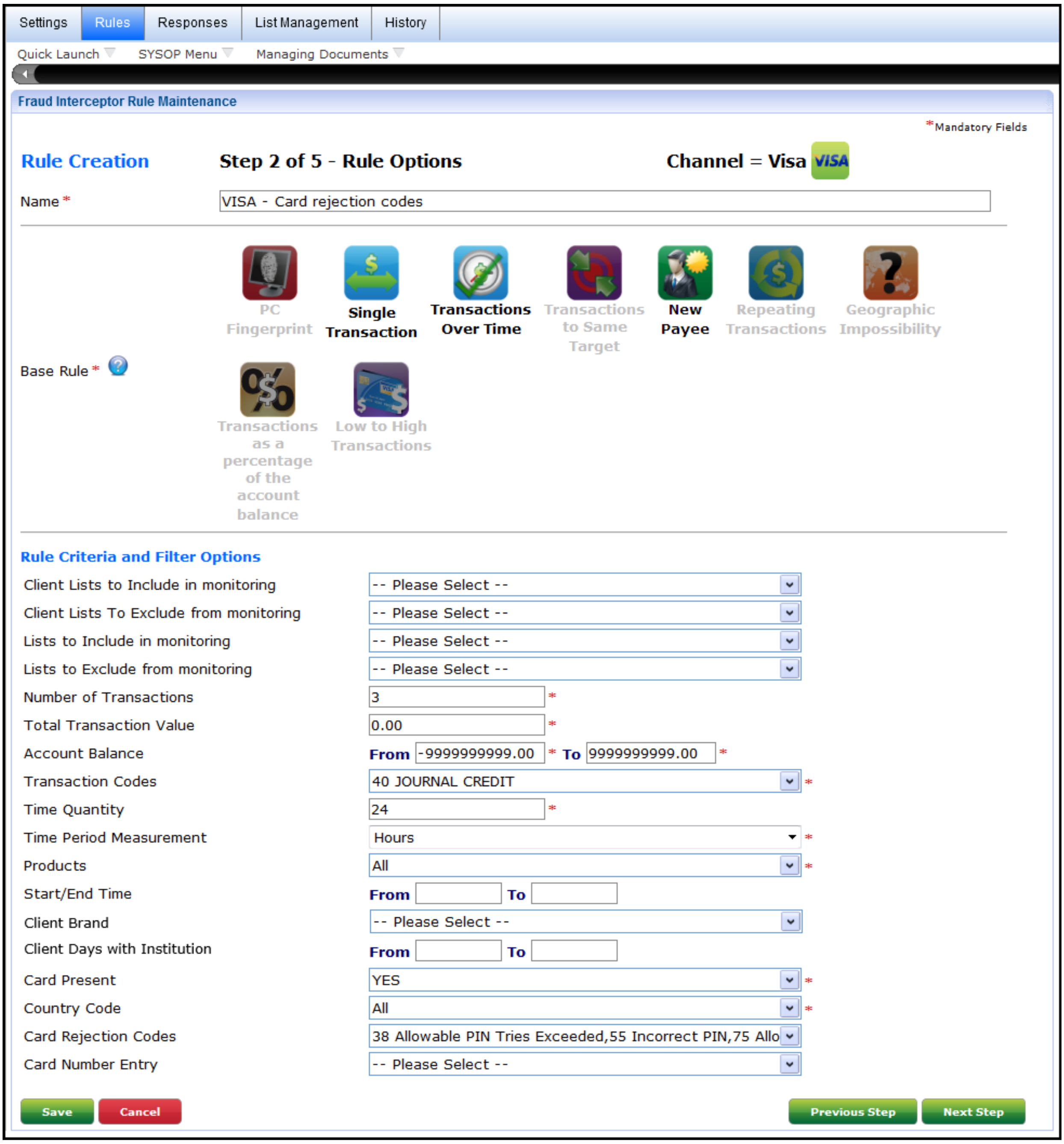
Name * VISA - Card rejection codes

Channel * Visa

Comments This rule is triggered for selected VISA channel card rejection codes.

This rule uses the VISA channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Visa**

Name * VISA - Card rejection codes

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	3 *
Total Transaction Value	0.00 *
Account Balance	From -9999999999.00 * To 9999999999.00 *
Transaction Codes	40 JOURNAL CREDIT *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Card Present	YES *
Country Code	All *
Card Rejection Codes	38 Allowable PIN Tries Exceeded,55 Incorrect PIN,75 Allo
Card Number Entry	-- Please Select --

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	There are no lists selected in this example; however, you could use client and other lists to suit your needs; for example, you could use a client list to exclude clients you know are low risk and frequently have a transaction pattern that would falsely trigger this rule.

Number of Transactions	If you enter '3' into this field, there must be at least three transactions within the specified time period.
Total Transaction Value	As these transactions will be rejected, they will have a zero value. Enter 0.00 into this field.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	This rule should only be looking for transaction narratives associated with card rejection codes. Therefore, the only transaction code that may be used is 40. Transaction code 40 is also used for non-value transactions.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected, however you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two VISA credit and debit products, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new VISA credit or debit products are created.
Start/End Time	These fields would normally be left blank in this rule to enable the rule to operate 24 hours a day.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Card Present	As this rule relates to PIN transactions, the card must be present. By selecting 'Yes' you are indicating that the card must be present.
Country Code	By selecting 'All' every country is included.
Card Rejection Codes	Card rejection codes to be included. Select 'All' for every card rejection code, or select one or more individual codes. Only the selected code values will be examined with this rule. In this example, the rejection codes for Allowable PIN Tries Exceeded, Incorrect PIN, and Allow No Of PIN Tries Exceeded have been selected.
Card Number Entry	The method by which the card number is acquired. This field is not mandatory. The field has been left blank as the source of the card number is not important in this example (the Card Present field covers what is required in this example).

ATM Channel Rules

The following examples cover a number of scenarios that may be useful for monitoring ATM transactions.

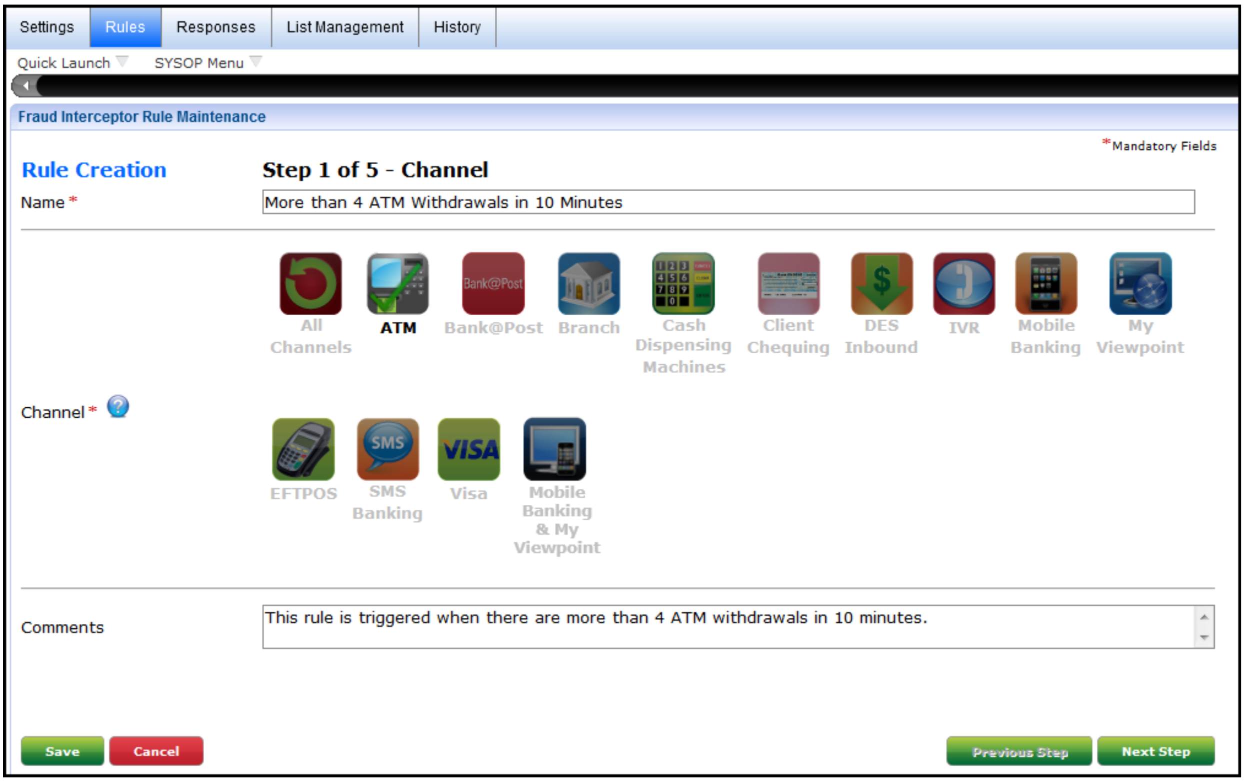
- More than four ATM withdrawals in 10 minutes
- More than one ATM card present transaction to the same payee over $5,000 in seven days

More than four ATM withdrawals in 10 minutes

This rule is triggered when more than four ATM card present transactions are triggered within 10 minutes.

This type of rule can be used to detect an unusually large number of transactions in a short time. As such, the value of the transactions and total value may be set to a very low figure.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



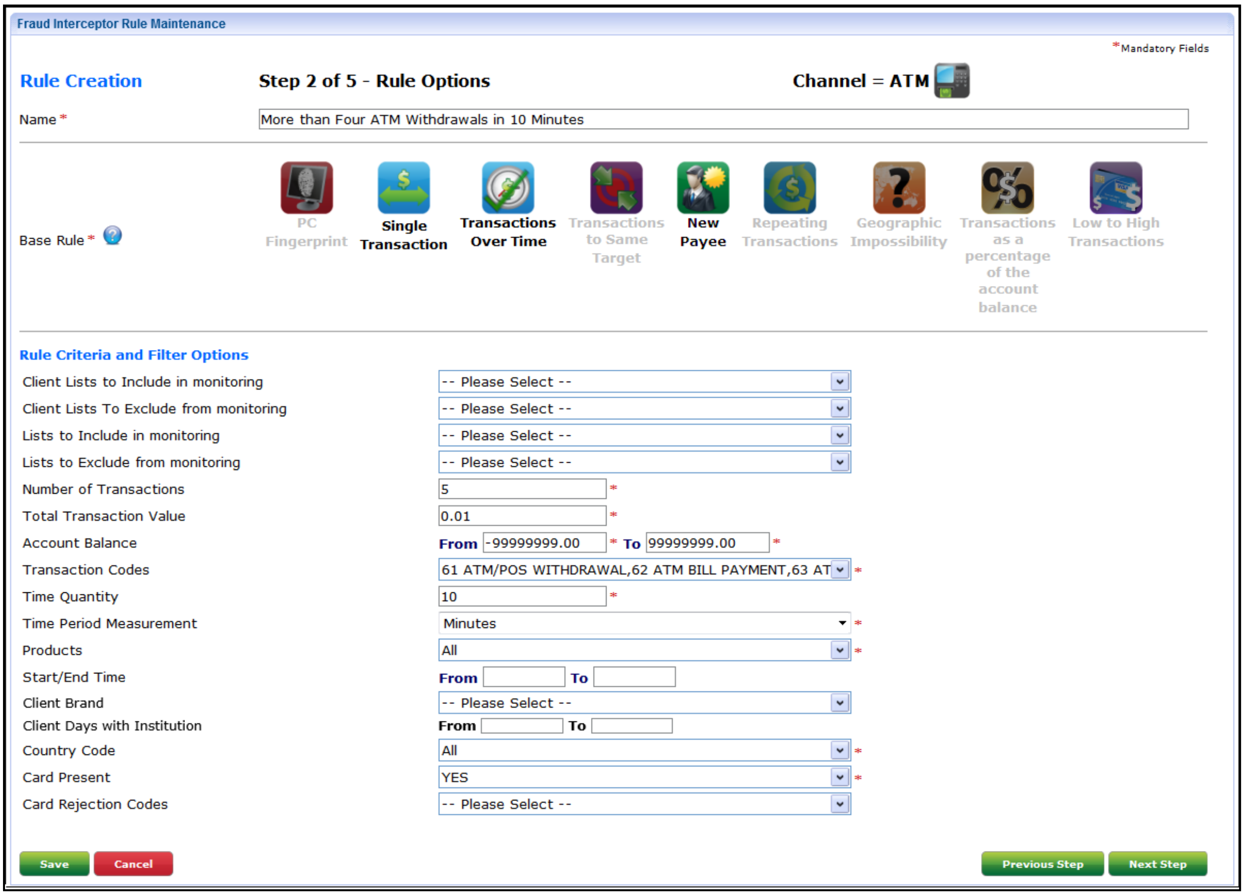
Name *: More than 4 ATM Withdrawals in 10 Minutes

Channel *: ATM

Comments: This rule is triggered when there are more than 4 ATM withdrawals in 10 minutes.

This rule uses the ATM Channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation — **Step 2 of 5 - Rule Options** — **Channel = ATM**

Name *	More than Four ATM Withdrawals in 10 Minutes
Base Rule *	Transactions Over Time

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	5 *
Total Transaction Value	0.01 *
Account Balance	From -99999999.00 * To 99999999.00 *
Transaction Codes	61 ATM/POS WITHDRAWAL,62 ATM BILL PAYMENT,63 AT *
Time Quantity	10 *
Time Period Measurement	Minutes *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Country Code	All *
Card Present	YES *
Card Rejection Codes	-- Please Select --

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	There are no lists selected in this example; however, you could use client and other lists to suit your needs; for example, you could use a client list to exclude clients you know are low risk and frequently have a transaction pattern that would falsely trigger this rule.
Number of Transactions	Enter '5' into this field to ensure there are more than transactions within the specified time period to trigger the rule.
Total Transaction Value	The total value of transactions is not important to this rule therefore a nominal value of $0.01 can be used.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	This rule only applies to ATM transactions so you can select the appropriate ATM transactions from the list. If you wanted, you could also select 'All' as this would have the same effect.

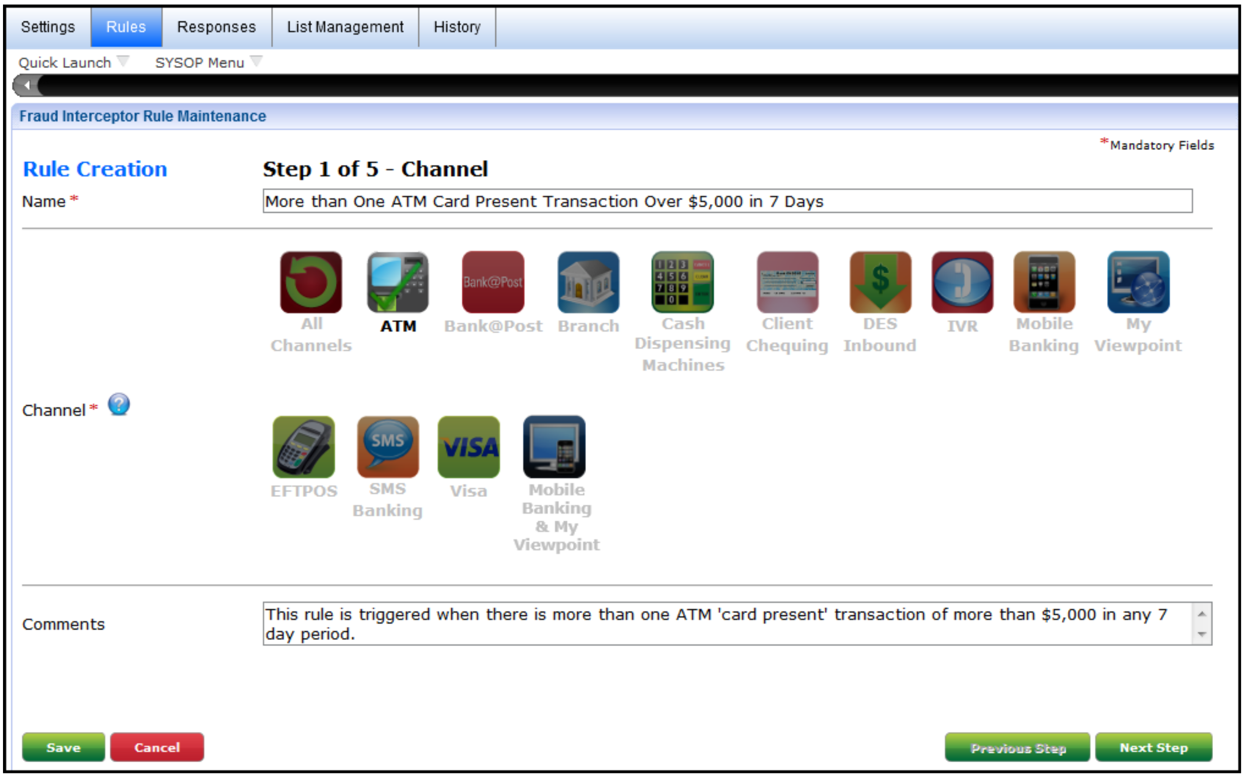
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '10' and 'Minutes' have been selected.
Products	'All' has been selected; however, if you only have one or two ATM card, you could select the individual products from the drop-down list. By selecting 'All' you will not have to update the rule when new card products are created.
Start/End Time	These fields would normally be left blank in this rule to enable the rule to operate 24 hours a day.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Country Code	By selecting 'All', every country is included. As this rule will apply only to ATM card present transactions and these can only be processed from Australia, you could have selected 'AUSTRALIA (AU)'.
Card Present	By selecting 'Yes' you are catering for personal transactions and are excluding telephone and Internet transactions.
Card Rejection Codes	Card rejection codes to be included. Select 'All' for every card rejection code, or select one or more individual codes. Only the selected code values will be examined with this rule.

More than one ATM card present transaction to the same payee over $5,000 in seven days

This rule is triggered when there is more than one high value ATM card present transaction to the same payee in a specified period. If dealing only with cash withdrawals from ATM machines, the value deemed "high value" will need to take into account the ATM cash transaction limit.

If other types of transaction are included (as in this example), you can set a higher value. It may even be appropriate to have separate rules for cash withdrawals and card purchases.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



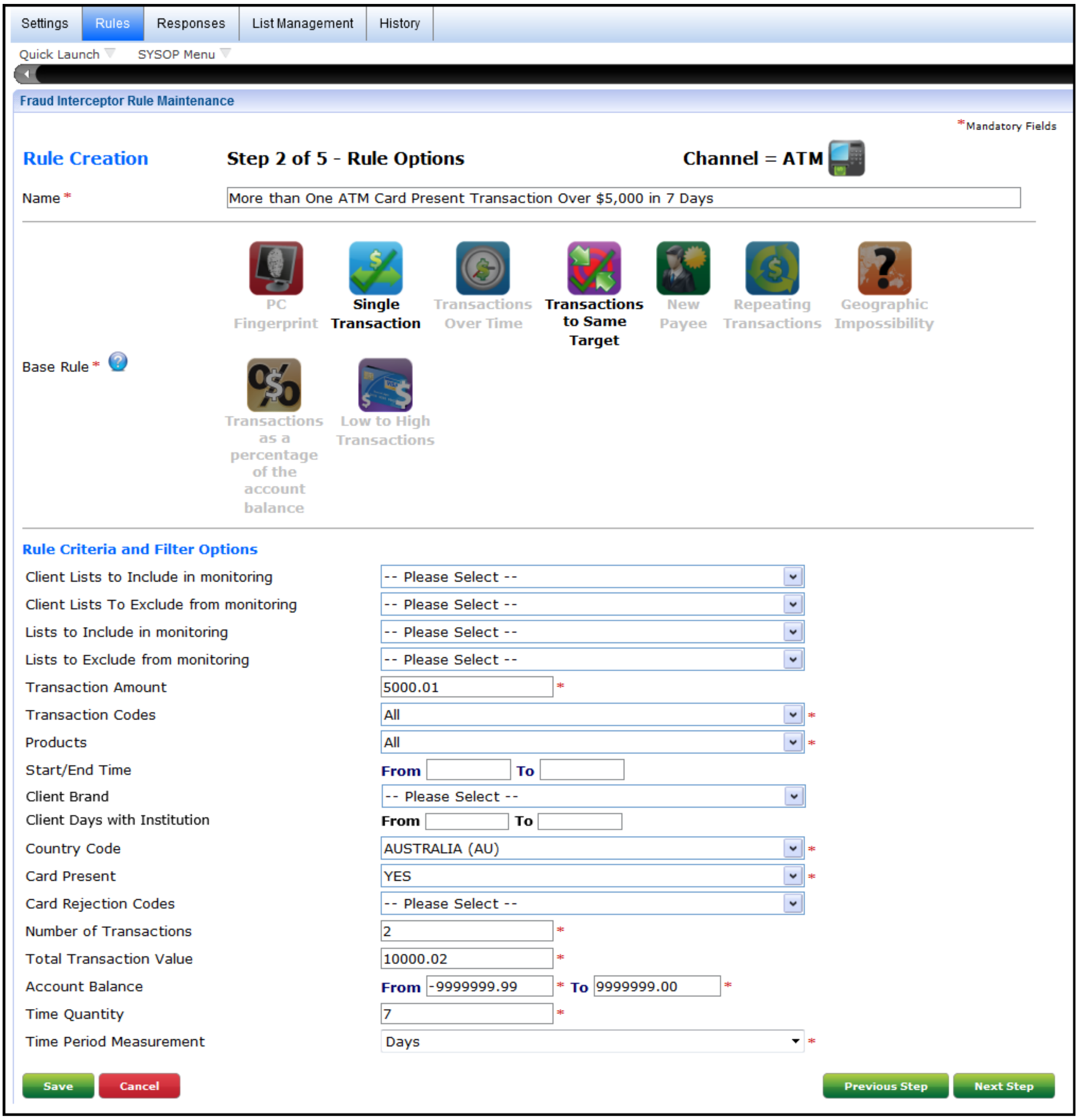
Name * More than One ATM Card Present Transaction Over $5,000 in 7 Days

Channel *

Comments: This rule is triggered when there is more than one ATM 'card present' transaction of more than $5,000 in any 7 day period.

This rule uses the ATM Channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation **Step 2 of 5 - Rule Options** **Channel = ATM**

Name * More than One ATM Card Present Transaction Over $5,000 in 7 Days

Base Rule * Single Transaction, Transactions to Same Target

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	5000.01 *
Transaction Codes	All *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Country Code	AUSTRALIA (AU) *
Card Present	YES *
Card Rejection Codes	-- Please Select --
Number of Transactions	2 *
Total Transaction Value	10000.02 *
Account Balance	From -9999999.99 * To 9999999.00 *
Time Quantity	7 *
Time Period Measurement	Days *

This rule uses the Base Rules 'Single Transaction' and 'Transactions to Same Target'. You need to use the Single Transaction Rule as having a total of transactions over $10,000 means that two transactions of $4,000 and $5,001 would also satisfy the total of transactions over time.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	Lists have not been used with this rule as you wish to target all transactions.

Transaction Amount	For this scenario, each transaction must be over $5,000, therefore $5,000.01 is the appropriate value for the Transaction Amount field.
Transaction Codes	Select the appropriate transaction codes. In this example, 'All' has been used. You could have selected only the codes relevant to ATM cards; however, the "Card Only" setting should ensure transactions will not be targeted.
Products	'All' has been selected; however, if you only have one or two products types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new ATM card products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Country Code	By selecting 'All', every country is included. As this rule will apply only to ATM card present transactions and these can only be processed from Australia, you could select 'AUSTRALIA (AU)'.
Card Present	This field must be set to 'YES' as only card present transactions are to be considered.
Card Rejection Codes	Card rejection codes to be included. Select 'All' for every card rejection code, or select one or more individual codes. Only the selected code values will be examined with this rule.

Card Number Entry

The method by which the card number is acquired.

This allows you to differentiate Rules based upon how the card transaction was initiated, for example a Rule could be set up to monitor only PayWave transactions. Likewise a Rule could be set up to monitor all transactions except chip initiated.

If the Card Present option is used, this will negate selections in Card Number Entry that conflict. For example if the Card Present is set to "No" and the Card Number Entry is set to "Chip" the Rule will not find any transactions as no Chip initiated transactions are Card Not Present. The below table shows the relationship between Card Number Entry and Card Present.

Card Number Entry	Card Present	Card Number Entry	Card Present
Bar Code	No	In-App	No
Chip	Yes	In-App - Android Pay	No
Contactless - FITBIT Pay	Yes	In-App - Apple Pay	No
Contactless - Garmin Pay	Yes	In-App - Garmin Pay	No
Contactless – Android Pay	Yes	In-App - Samsung Pay	No
Contactless – Apple Pay	Yes	In-App FITBIT Pay	No
Contactless – Card/Pay/Way	Yes	Integrated Circuit Card:Limited	Yes
Contactless – Magnetic Stripe	Yes	Key Entered Input	No
Contactless – Manual Entry	No	Magnetic Stripe	Yes
Contactless – Samsung Pay	Yes	Magnetic Stripe (90)	Yes
Contactless Card:Limited	No	Manual	No
Contactless Magnetic	No	OCR	No
Contactless Using Magnetic Stripe	No	PAN Auto Entry Via Server	No
Credentials On File	No	Stored Value	Yes
Electronic Commerce	No	Unspecified	No
Fallback	Yes		

The card number entry methods that are available for your financial institution may differ, depending on your switching service provider.

Number of Transactions	The scenario is triggered when '2' transactions of more than $5,000 each occur within the specified timeframe.
Total Transaction Value	This rule is triggered when the transactions total more than $10,000 so 10000.01 is an appropriate value for this field.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '7' and 'Days' have been selected.

Cyber Breaches

Cyber breaches are a serious problem and becoming more frequent, affecting individuals, businesses and, in particular, financial institutions.

Fraud Interceptor can be used to help mitigate cyber security issues for your financial institutions clients.

With Fraud Interceptor, the suggested overall approach to cyber breaches is layered and comprises three aspects:

- **Global level** – broad rule to focus on either client advice lists or compromised card lists
- **Channel level** – specific rules on card behaviour transactions – small to large transactions
- **List level** – compromised card lists and how many and how quickly they can be imported.

The details below give step-by-step examples of how to set up these layers of cyber protection, with the focus on cyber crime where card data is known to have been shared.

Setting up lists

The cyber breach-specific rules, to be set up in later steps described below, will work with these two lists:

- **Clients Impacted by Cyber Breach** - this can be set up manually.
- **Compromised Cards** - this can be a simple list of card numbers, imported from a '.csv' file.

Fraud Lists are lists of information that may be used by Fraud Rules to include or exclude transaction

matches in association with the Rule to which the List is applied. The Fraud Lists contain different types of

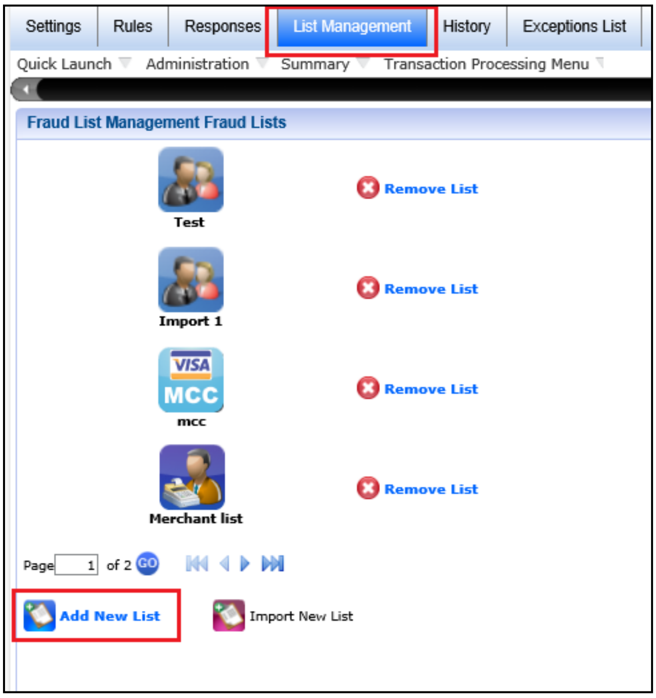
information based on the List Type, and effectively allow Rules to be fine-tuned.

Below is an outline of the process for setting up lists. If you already have these lists set up, go to the **Setting up Rules** section below.

Refer to the **What are Fraud Lists?** section of the *Fraud Interceptor User Manual* for full details.

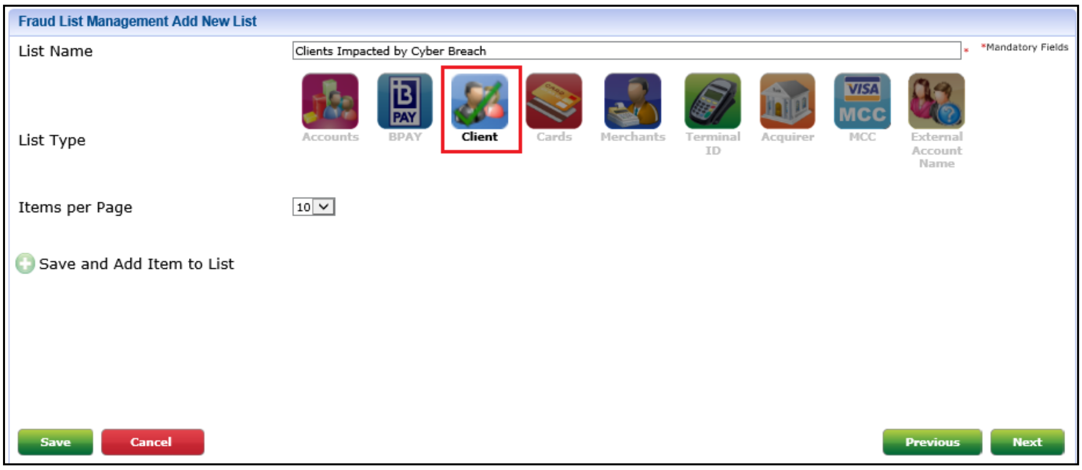
Step 1 Go to the **Fraud Interceptor Settings** page then click the **List Management** tab.

Step 2 Click on the **Add New List** link:



Step 3 Enter a descriptive name in the **List Name** field.

Step 4 Click on the Client icon for **List Type**.



List Name: Clients Impacted by Cyber Breach *

List Type: Client

Items per Page: 10

Step 5 Click the ➕ **Save and Add Item to List** link to go to the page where the list can be populated.

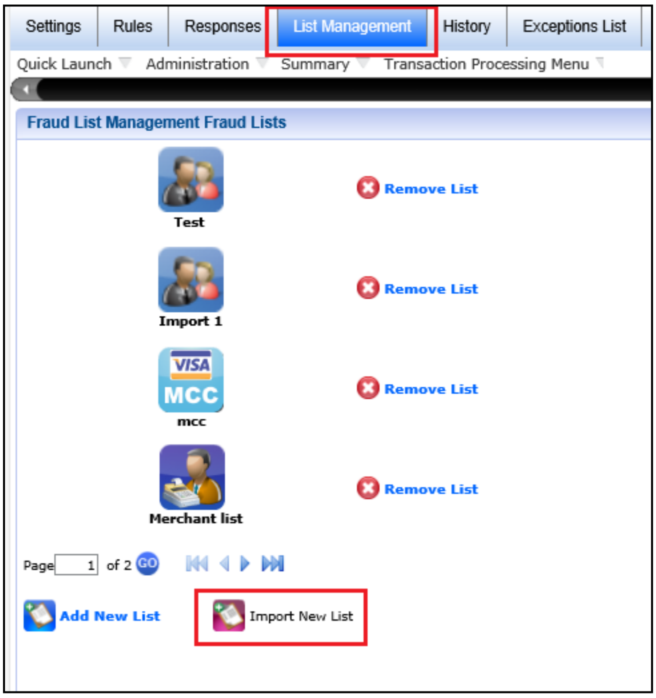
Refer to the **Add items to your List** section of the *Fraud Interceptor User Manual* for full details on how to add entries to your list.

Step 6 When all required entries have been added to the list, click the green **Save** button located at the bottom left of the page to complete the process.

Repeat a similar process to set up a **Compromised Cards** list but this time it will involve importing a file of card information.

Step 1 Go to the **Fraud Interceptor Settings** page then click the **List Management** tab.

Step 2 Click on the **Import New List** link:

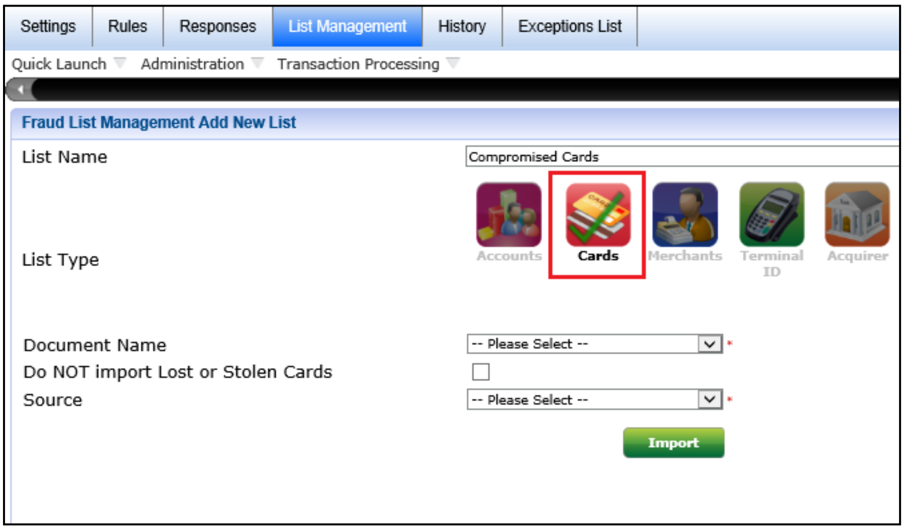


You can import Card lists using comma-separated values (CSV) files.

You can import a CSV file to create a new list, as well as importing a CSV file to add items to an existing List or replace the items in an existing list.

Step 3 Enter a descriptive name in the **List Name** field.

Step 4 Click on the **Cards** icon for **List Type**.



List Name: Compromised Cards

List Type: Cards

Document Name: -- Please Select -- *

Do NOT import Lost or Stolen Cards: □

Source: -- Please Select -- *

Step 5 Complete the fields to specify the file to be imported.

Step 6 Click **Import**.

Refer to the **Add items to your List** section of the *Fraud Interceptor User Manual* for more details.

Step 7 When all required entries have been added to the list, click the green **Save** button located at the bottom left of the page to complete the process.

Setting up Rules

Below is an outline of the process, highlighting the key relevant settings.

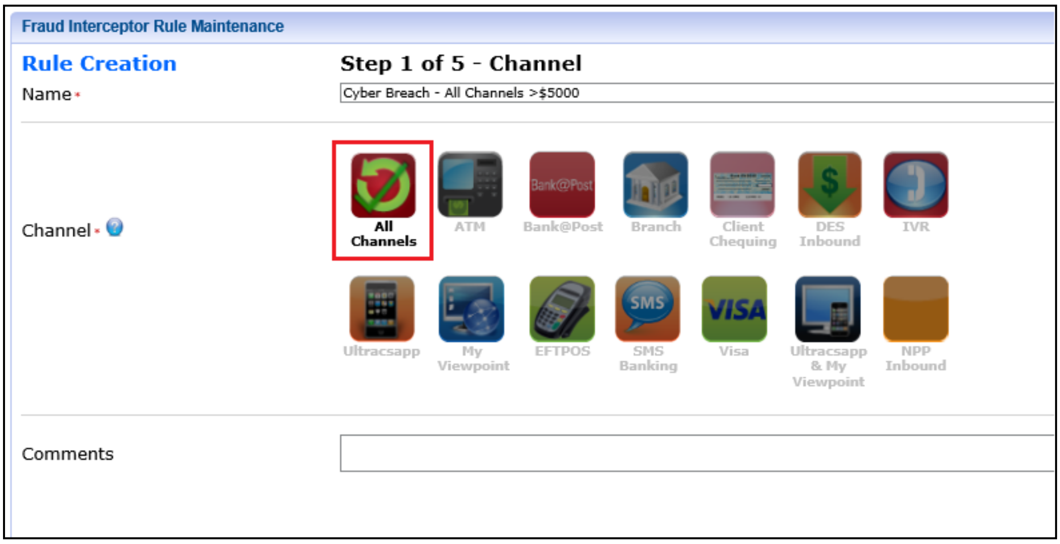
Refer to the *Fraud Interceptor User Manual* for full details of the five steps involved.

Global Level

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - All Channels >$5000' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **All Channels** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

Name* Cyber Breach - All Channels >$5000

Channel* All Channels

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

This rule is used to determine any transaction greater than $5000 that is processed from a Clients Impacted by Cyber Breach list or Compromised Cards list.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

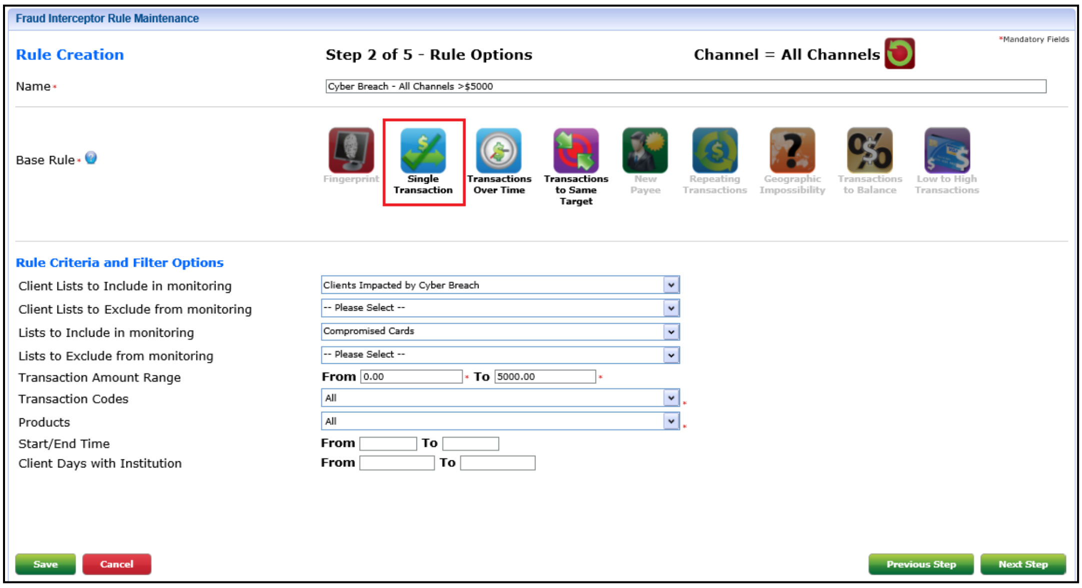
Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Compromised Cards** list from the drop-down options.

Step 2d Enter a **Transaction Amount Range** of '0.00' to '5000.00'.

Step 2e Select 'All' for the mandatory **Transaction Codes** and **Products** fields.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 2 of 5 - Rule Options

Channel = All Channels

Name*: Cyber Breach - All Channels >$5000

Base Rule*: Single Transaction

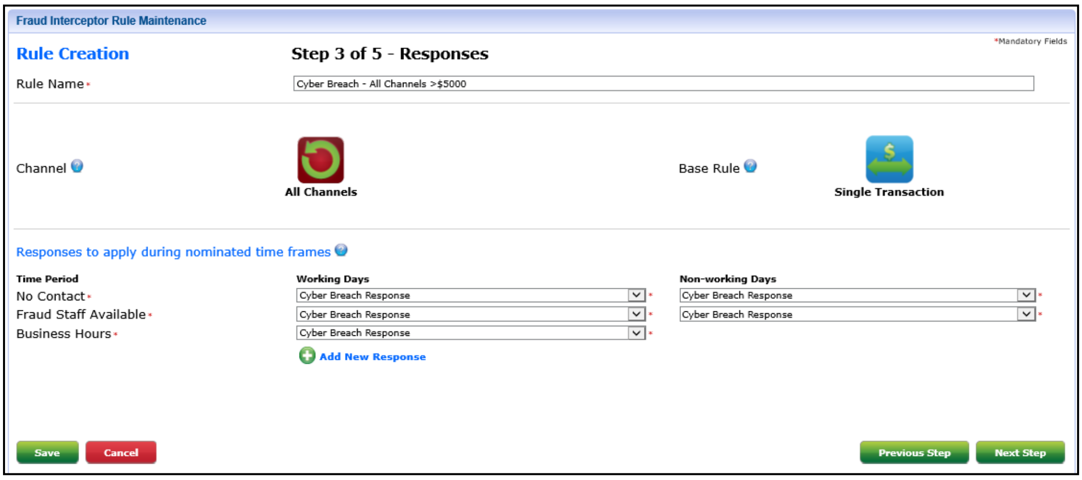
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists to Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Compromised Cards
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 0.00* To 5000.00*
Transaction Codes	All*
Products	All*
Start/End Time	From To
Client Days with Institution	From To

Step 2f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following same Response from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation Step 3 of 5 - Responses

*Mandatory Fields

Rule Name* Cyber Breach - All Channels >$5000

Channel: All Channels

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Cyber Breach Response*	Cyber Breach Response*
Fraud Staff Available*	Cyber Breach Response*	Cyber Breach Response*
Business Hours*	Cyber Breach Response*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

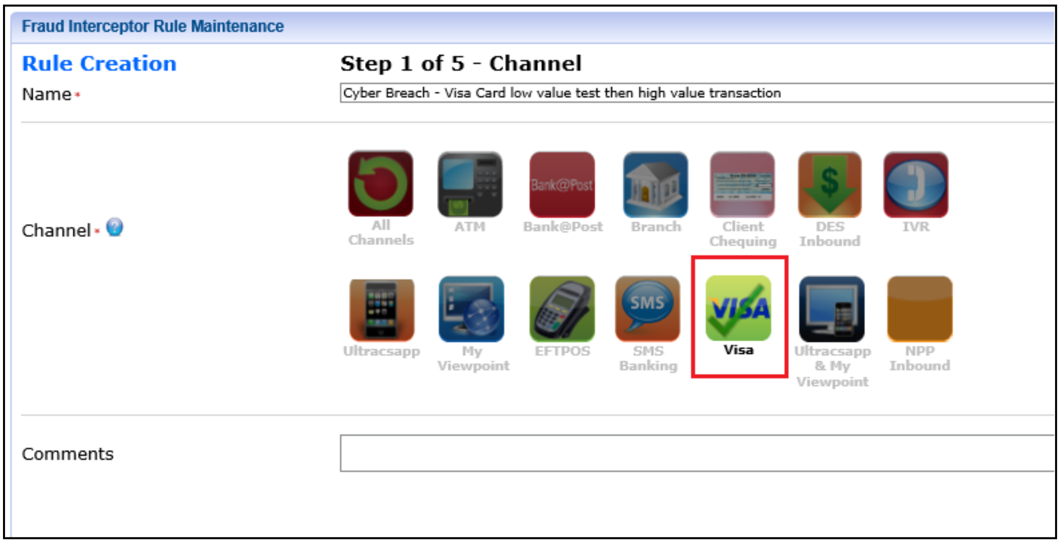
If required, click the **Previous Step** button go back to earlier steps.

Channel Level

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - Visa Card low value test then high value transaction' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

Name*: Cyber Breach - Visa Card low value test then high value transaction

Channel*

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

Used to identify suspicious activity where the fraudster first performs a low value transaction, typically less than $9.99 and then within 10 minutes performs a high value transaction over $1000

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Low to High Transactions** icon.

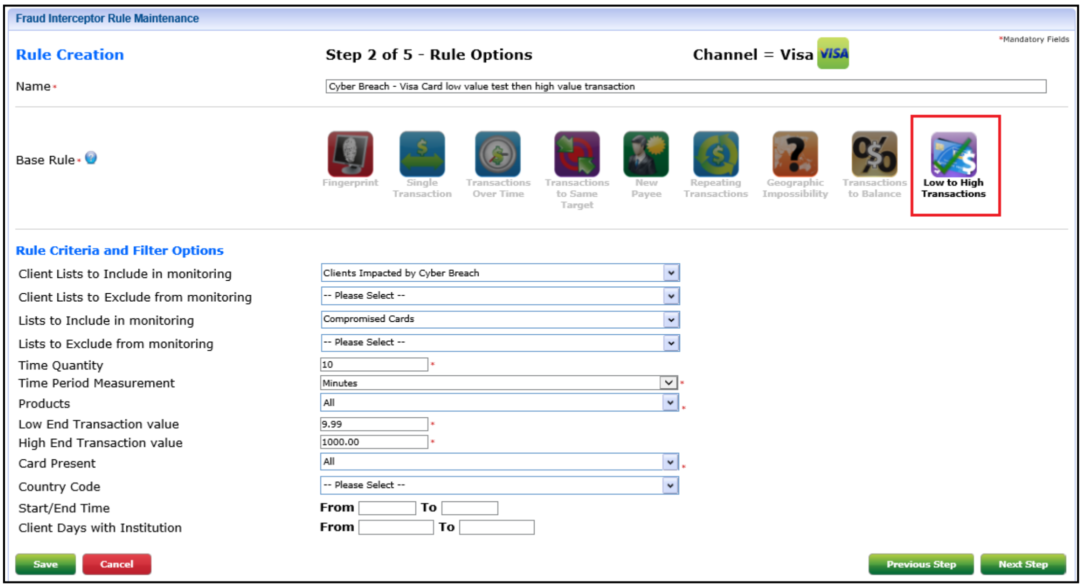
Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Compromised Cards** list from the drop-down options.

Step 2d Enter '10' in the **Time Quantity** field and select **Minutes** from the drop-down options for the **Time Management Measurement** field.

Step 2e Select 'All' for the mandatory **Products** and **Card Present** fields.

Step 2f Enter '9.99' in the **Low End Transaction value** field and enter '1000.00' in the **High End Transaction value** field.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation — Step 2 of 5 - Rule Options — Channel = Visa

Name* Cyber Breach - Visa Card low value test then high value transaction

Base Rule*

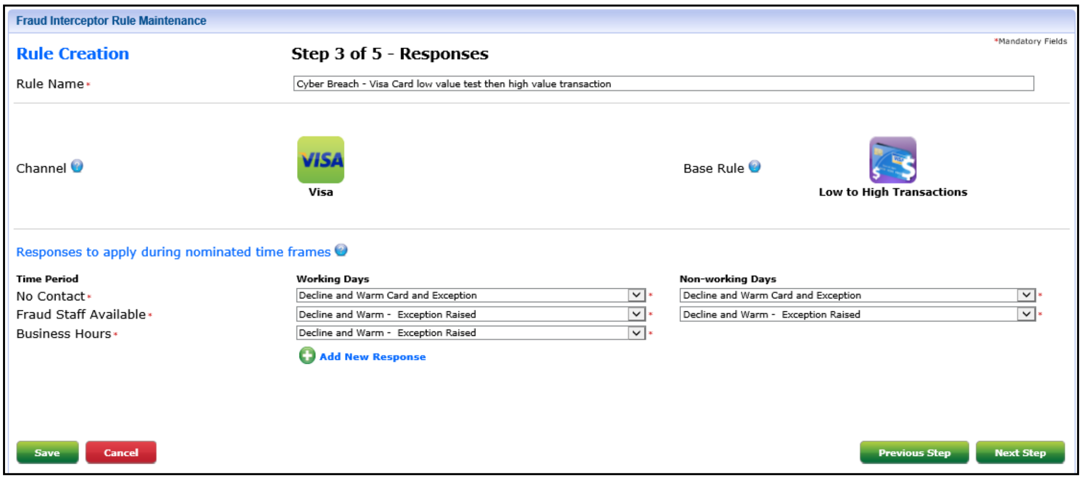
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists to Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Compromised Cards
Lists to Exclude from monitoring	-- Please Select --
Time Quantity	10 *
Time Period Measurement	Minutes *
Products	All *
Low End Transaction value	9.99 *
High End Transaction value	1000.00 *
Card Present	All *
Country Code	-- Please Select --
Start/End Time	From To
Client Days with Institution	From To

Step 2g Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following Responses from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation Step 3 of 5 - Responses

*Mandatory Fields

Rule Name* Cyber Breach - Visa Card low value test then high value transaction

Channel: Visa

Base Rule: Low to High Transactions

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Decline and Warm Card and Exception*	Decline and Warm Card and Exception*
Fraud Staff Available*	Decline and Warm - Exception Raised*	Decline and Warm - Exception Raised*
Business Hours*	Decline and Warm - Exception Raised*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

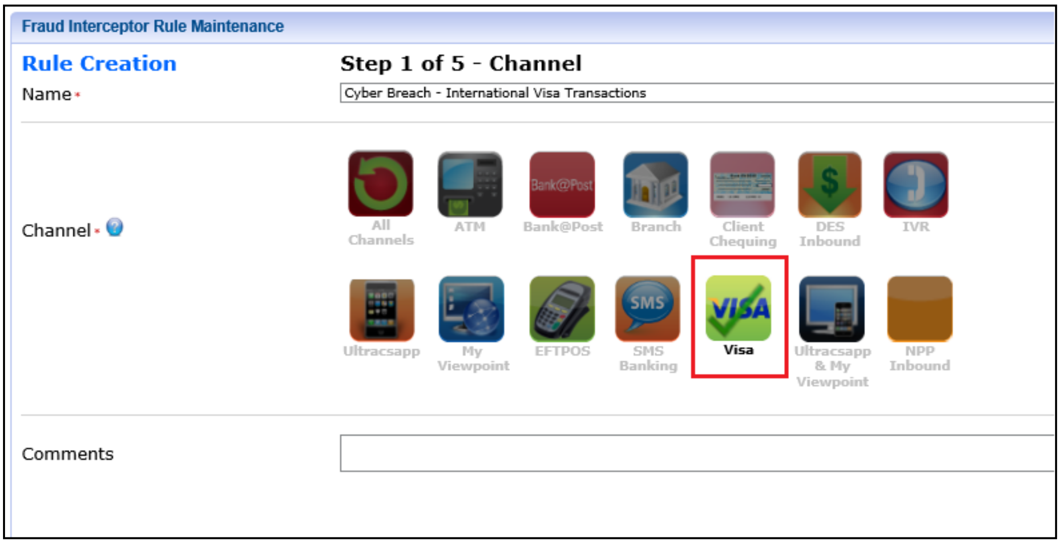
If required, click the **Previous Step** button go back to earlier steps.

International Visa Transactions

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - International Visa Transactions' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

Name* Cyber Breach - International Visa Transactions

Channel*

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

All international transactions on imported Compromised Cards list or Clients Impacted by Cyber Breach list declined.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Compromised Cards** list from the drop-down options.

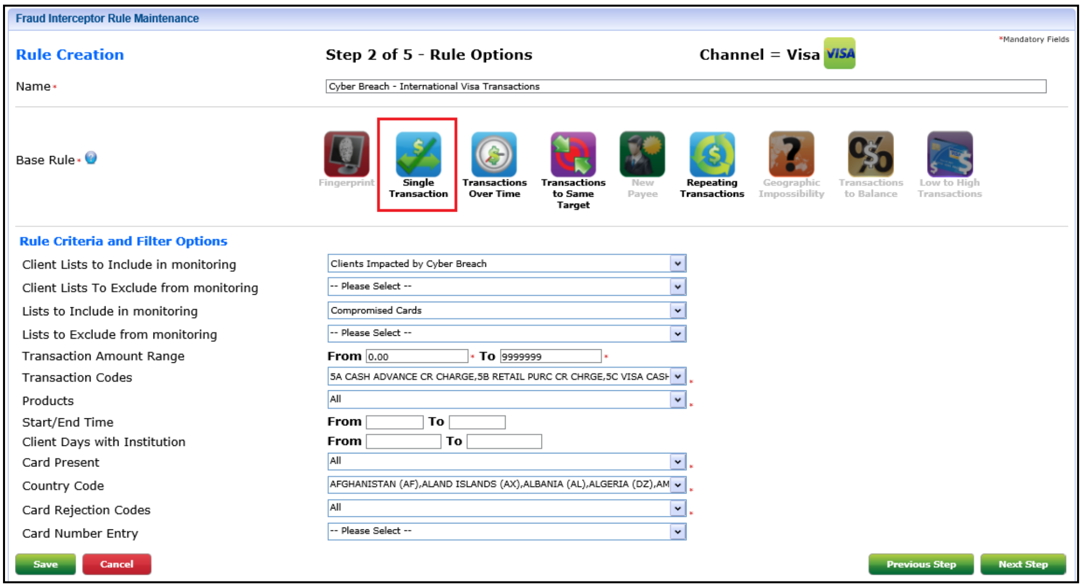
Step 2d For the **Transaction Amount Range** fields, enter **From** '0.00' **To** '9999999'.

Step 2e Select the appropriate **Transaction Codes** from the drop-down list.

Step 2f Select 'All' for the mandatory **Products**, **Card Present** and the **Card Rejection Codes** fields.

Step 2g Select all countries *other than your own*.

The easiest way to do this is to select the 'All' option from the drop-down list and then deselect your own country.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation — Step 2 of 5 - Rule Options — Channel = Visa

Name*	Cyber Breach - International Visa Transactions
Base Rule*	Single Transaction

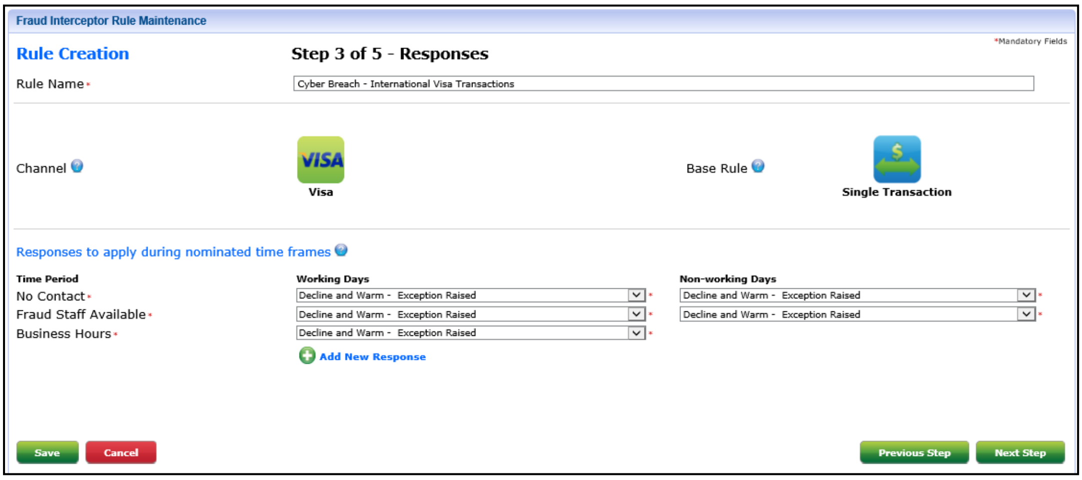
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Compromised Cards
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 0.00 * To 9999999 *
Transaction Codes	5A CASH ADVANCE CR CHARGE,5B RETAIL PURC CR CHRGE,5C VISA CASH *
Products	All *
Start/End Time	From To
Client Days with Institution	From To
Card Present	All *
Country Code	AFGHANISTAN (AF),ALAND ISLANDS (AX),ALBANIA (AL),ALGERIA (DZ),AM *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

Step 2h Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following same Response from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation

Step 3 of 5 - Responses

*Mandatory Fields

Rule Name* Cyber Breach - International Visa Transactions

Channel: Visa

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Decline and Warm - Exception Raised *	Decline and Warm - Exception Raised *
Fraud Staff Available*	Decline and Warm - Exception Raised *	Decline and Warm - Exception Raised *
Business Hours*	Decline and Warm - Exception Raised *	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

Cyber Breach - Ticketmaster example

Personal and Card Payment details stolen

The hacker group ShinyHunters allegedly breached Ticketmaster’s data in late May 2024, including obtaining the **credit and debit card information** of over 560 million consumers worldwide.

Fraud Interceptor can be used to help mitigate cyber security issues for your clients following this type of breach.

With Fraud Interceptor, the suggested overall approach to cyber breaches is layered and comprises three aspects:

- **Global level** – broad rule to focus on either client advice lists or compromised card lists
- **Channel level** – specific rules on card behaviour transactions – small to large transactions
- **List level** – compromised card lists and how many and how quickly they can be imported.

The details below give step-by-step examples of how to set up these layers of cyber protection, with the focus on cyber crime where card data is known to have been shared.

Setting up lists

The cyber breach-specific rules, to be set up in later steps described below, will work with two lists.:

- **Cyberbreach Clients List** - this can be set up manually.
- **Compromised Card List** - this can be a simple list of card numbers, imported from a '.csv' file.

(Example names only. You can enter a specific descriptive name in the **List Name** field when setting up the list.)

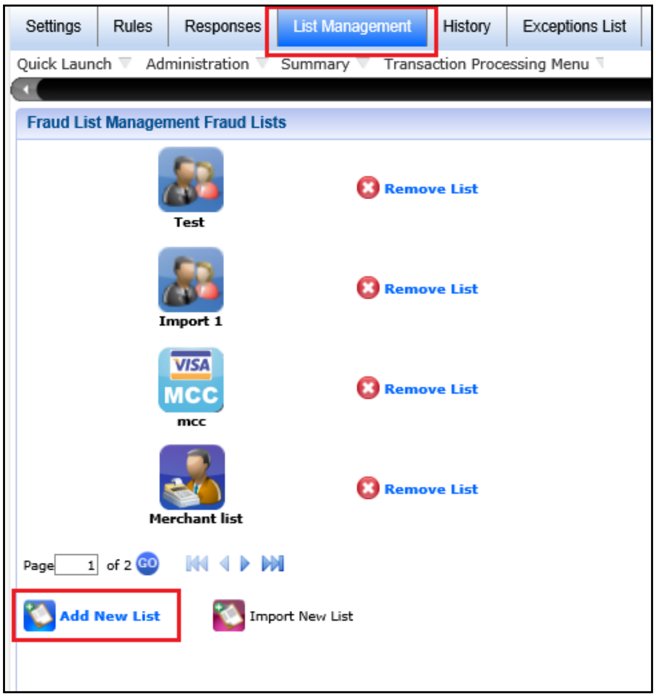
> Fraud Lists are lists of information that may be used by Fraud Rules to include or exclude transaction
>
> matches in association with the Rule to which the List is applied. The Fraud Lists contain different types of
>
> information based on the List Type, and effectively allow Rules to be fine-tuned.

Below is an outline of the process for setting up lists. If you already have these lists set up, go to the **Setting up Rules** section below.

Refer to the **What are Fraud Lists?** section of the *Fraud Interceptor User Manual* for full details.

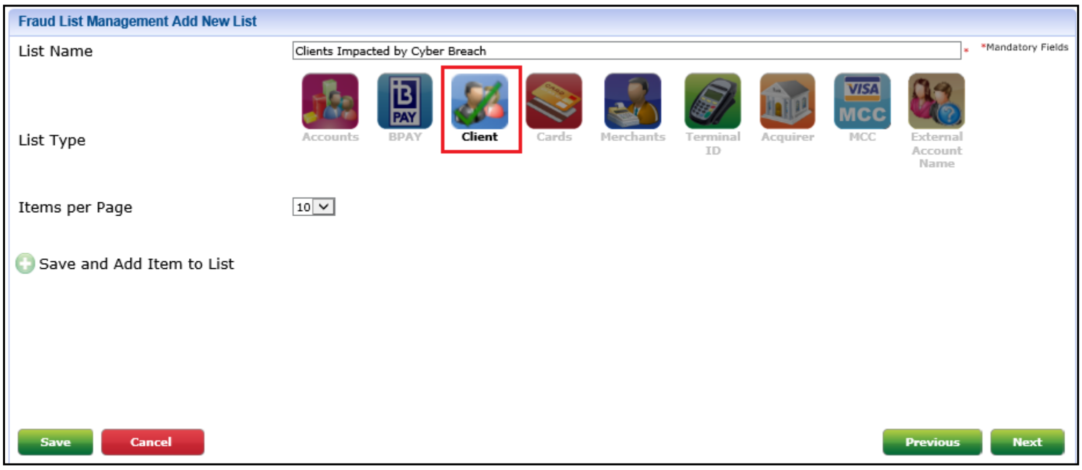
Step 1 Go to the **Fraud Interceptor Settings** page then click the **List Management** tab.

Step 2 Click on the **Add New List** link:



Step 3 Enter a descriptive name in the **List Name** field.

Step 4 Click on the Client icon for **List Type**.


Fraud List Management Add New List

List Name: Clients Impacted by Cyber Breach *

Items per Page: 10

Step 5 Click the ➕ **Save and Add Item to List** link to go to the page where the list can be populated.

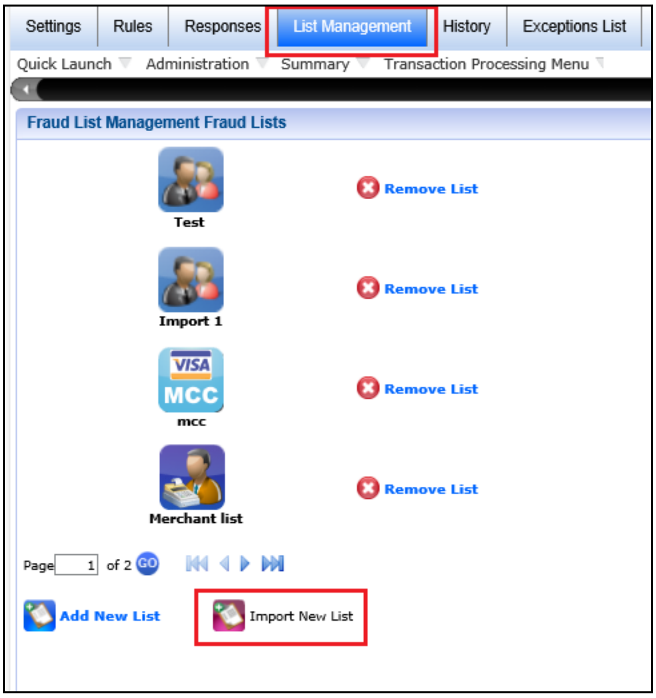
Refer to the **Add items to your List** section of the *Fraud Interceptor User Manual* for full details on how to add entries to your list.

Step 6 When all required entries have been added to the list, click the green **Save** button located at the bottom left of the page to complete the process.

Repeat a similar process to set up a **Compromised Cards** list but this time it will involve importing a file of card information.

Step 1 Go to the **Fraud Interceptor Settings** page then click the **List Management** tab.

Step 2 Click on the **Import New List** link:

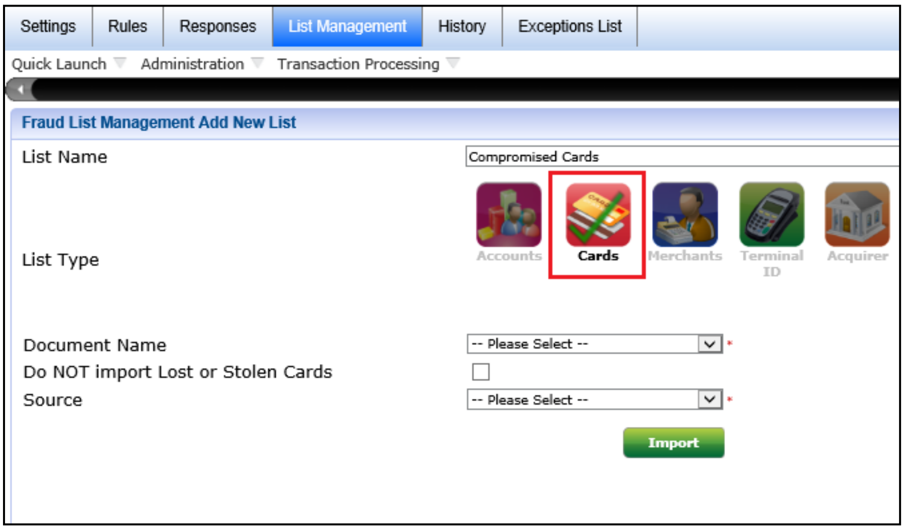


You can import Card lists using comma-separated values (CSV) files.

You can import a CSV file to create a new list, as well as importing a CSV file to add items to an existing List or replace the items in an existing list.

Step 3 Enter a descriptive name in the **List Name** field.

Step 4 Click on the **Cards** icon for **List Type**.



List Name: Compromised Cards

List Type: Cards

Document Name: -- Please Select -- *

Do NOT import Lost or Stolen Cards: □

Source: -- Please Select -- *

Step 5 Complete the fields to specify the file to be imported.

Step 6 Click **Import**.

Refer to the **Add items to your List** section of the *Fraud Interceptor User Manual* for more details.

Step 7 When all required entries have been added to the list, click the green **Save** button located at the bottom left of the page to complete the process.

Setting up Rules

Below is an outline of the process, highlighting the key relevant settings.

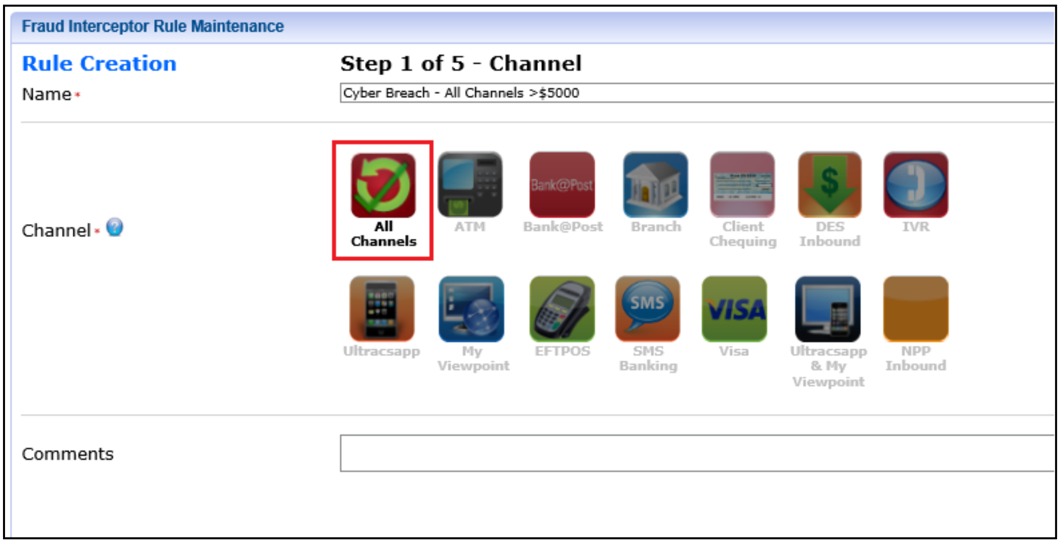
Refer to the *Fraud Interceptor User Manual* for full details of the five steps involved.

Global Level

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - All Channels >$5000' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **All Channels** icon.



Fraud Interceptor Rule Maintenance

Rule Creation — Step 1 of 5 - Channel

Name* Cyber Breach - All Channels >$5000

Channel* All Channels

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

This rule is used to determine any transaction greater than $5000 that is processed and involves entries from the Clients Impacted by Cyber Breach list or Compromised Cards list.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

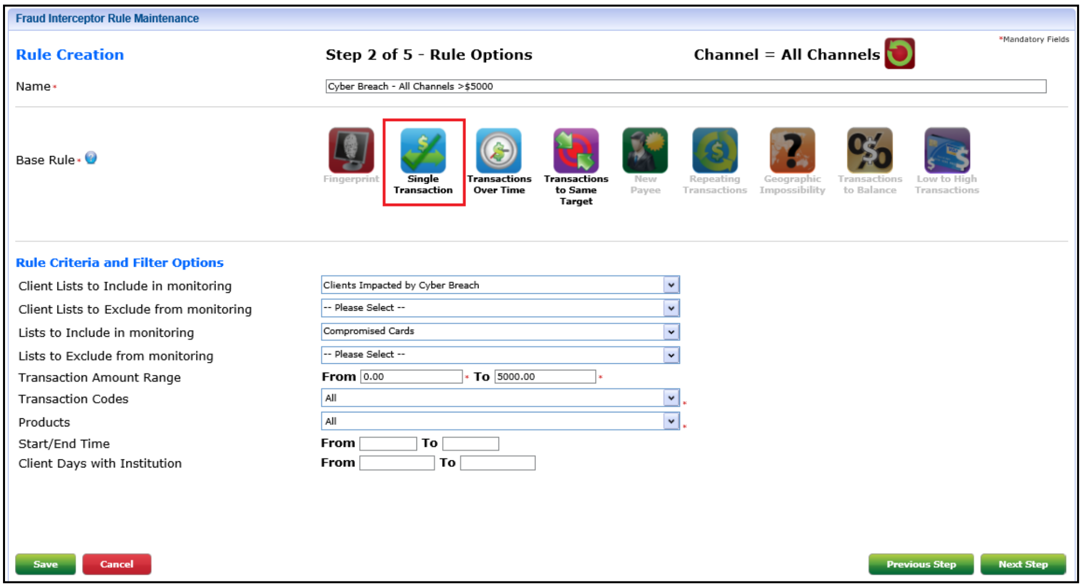
Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Compromised Cards** list from the drop-down options.

Step 2d Enter a **Transaction Amount Range** of '0.00' to '5000.00'.

Step 2e Select 'All' for the mandatory **Transaction Codes** and **Products** fields.



Rule Creation — Step 2 of 5 - Rule Options — Channel = All Channels

Name* Cyber Breach - All Channels >$5000

Base Rule*

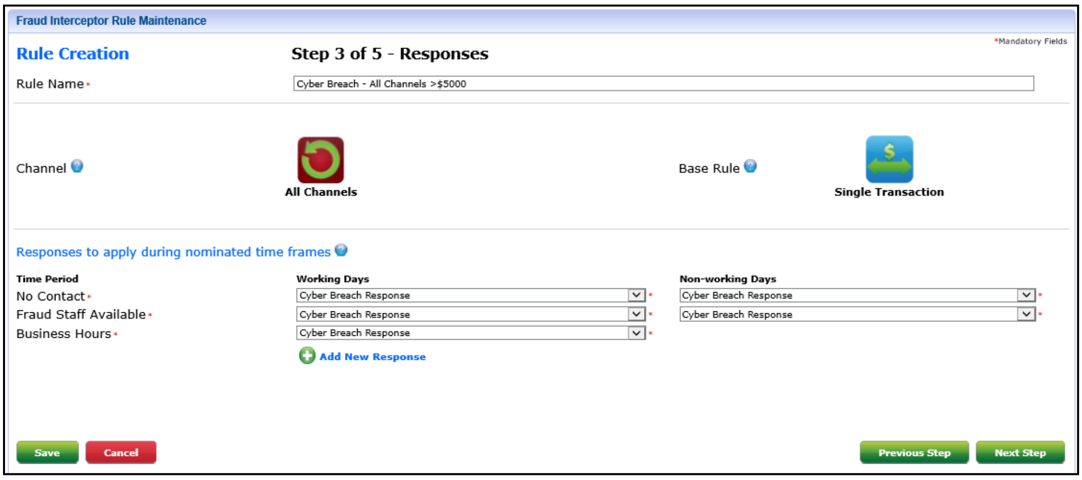
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists to Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Compromised Cards
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 0.00* To 5000.00*
Transaction Codes	All*
Products	All*
Start/End Time	From To
Client Days with Institution	From To

Step 2f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following same Response from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation

Step 3 of 5 - Responses

*Mandatory Fields

Rule Name* Cyber Breach - All Channels >$5000

Channel: All Channels

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Cyber Breach Response*	Cyber Breach Response*
Fraud Staff Available*	Cyber Breach Response*	Cyber Breach Response*
Business Hours*	Cyber Breach Response*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

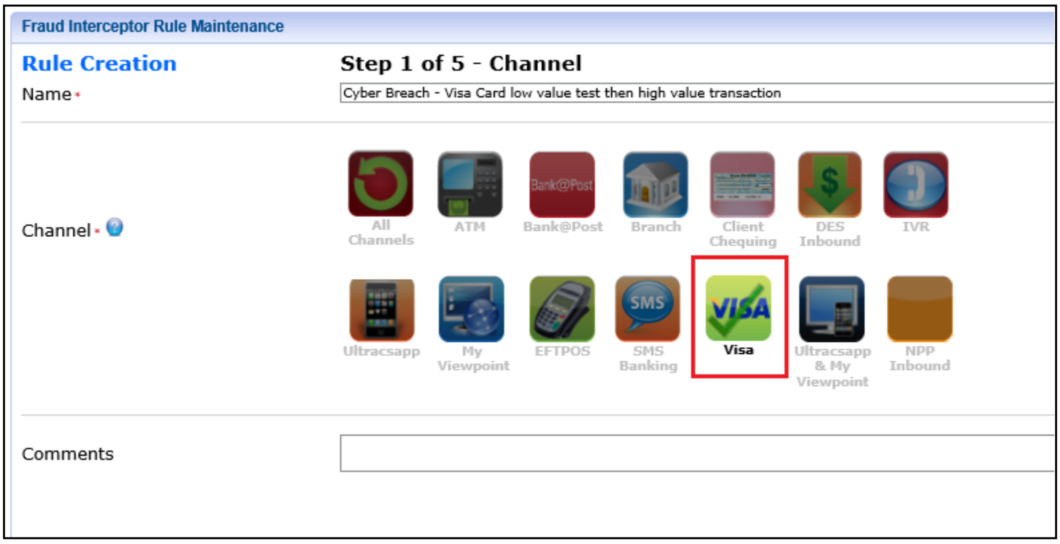
If required, click the **Previous Step** button go back to earlier steps.

Channel Level

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - Visa Card low value test then high value transaction' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

Name* Cyber Breach - Visa Card low value test then high value transaction

Channel*

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

Used to identify suspicious activity where the fraudster first performs a low value transaction, typically less than $9.99 and then within 10 minutes performs a high value transaction over $1000

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Low to High Transactions** icon.

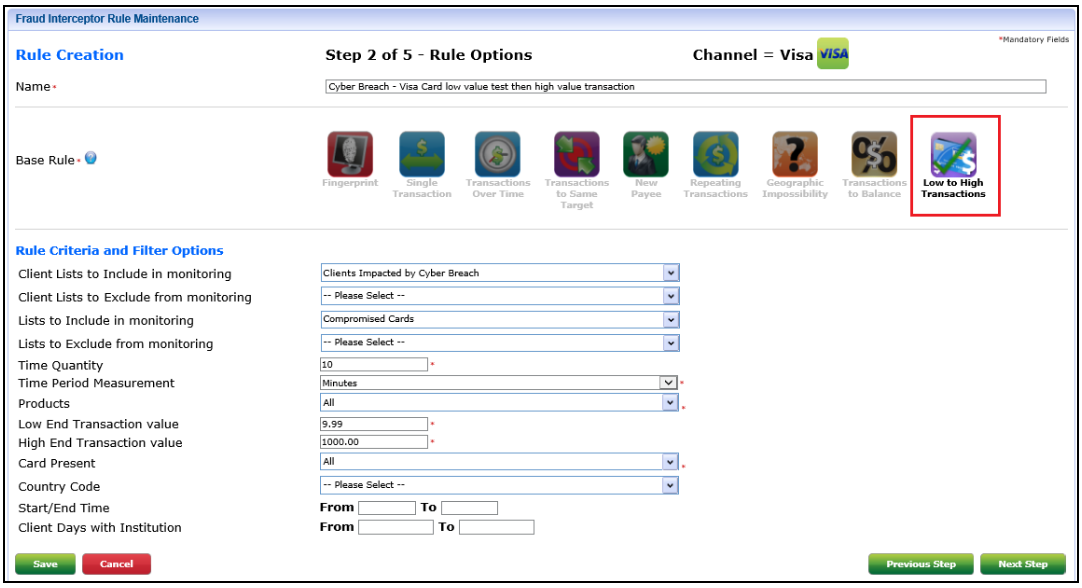
Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Compromised Cards** list from the drop-down options.

Step 2d Enter '10' in the **Time Quantity** field and select **Minutes** from the drop-down options for the **Time Management Measurement** field.

Step 2e Select 'All' for the mandatory **Products** and **Card Present** fields.

Step 2f Enter '0.99' in the **Low End Transaction value** field and enter '1000.00' in the **High End Transaction value** field.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation — Step 2 of 5 - Rule Options — Channel = Visa

Name*	Cyber Breach - Visa Card low value test then high value transaction
Base Rule*	Low to High Transactions

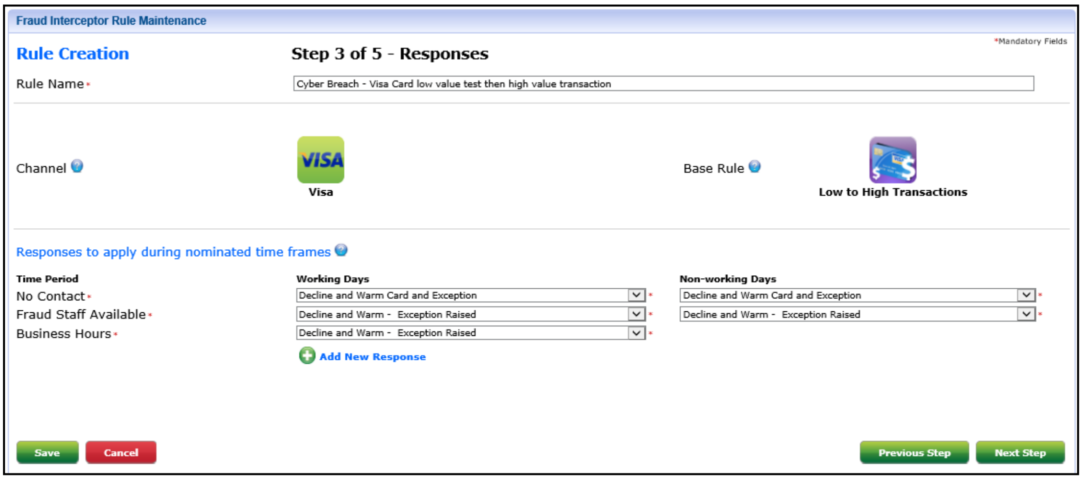
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists to Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Compromised Cards
Lists to Exclude from monitoring	-- Please Select --
Time Quantity	10 *
Time Period Measurement	Minutes *
Products	All *
Low End Transaction value	9.99 *
High End Transaction value	1000.00 *
Card Present	All *
Country Code	-- Please Select --
Start/End Time	From To
Client Days with Institution	From To

Step 2g Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following Responses from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation — **Step 3 of 5 - Responses**

*Mandatory Fields

Rule Name*: Cyber Breach - Visa Card low value test then high value transaction

Channel: Visa

Base Rule: Low to High Transactions

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Decline and Warm Card and Exception	Decline and Warm Card and Exception
Fraud Staff Available*	Decline and Warm - Exception Raised	Decline and Warm - Exception Raised
Business Hours*	Decline and Warm - Exception Raised	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

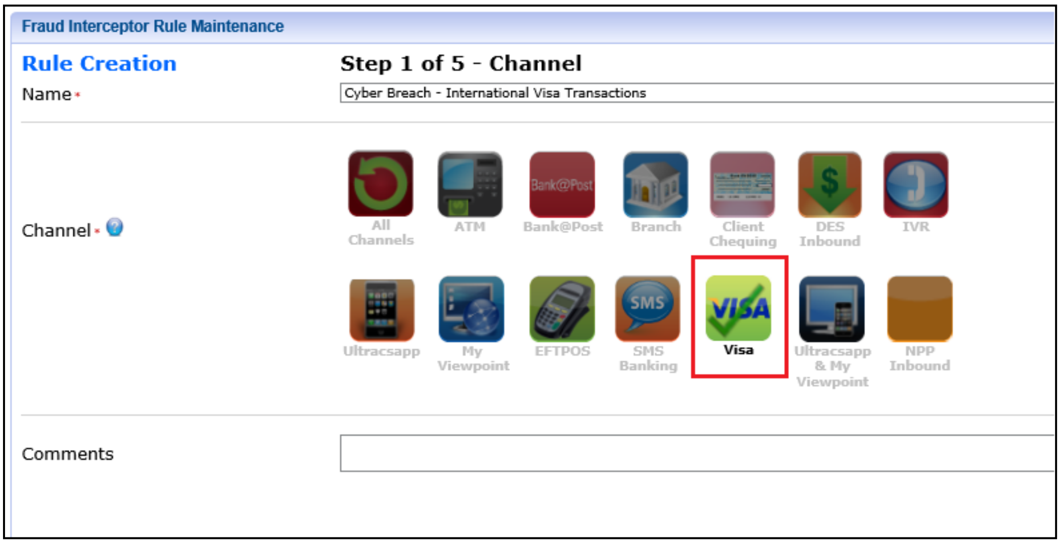
If required, click the **Previous Step** button go back to earlier steps.

International Visa Transactions

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyber Breach - International Visa Transactions' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

Name* Cyber Breach - International Visa Transactions

Channel*

Comments

Step 1d Type a descriptive entry into the **Comments** field, such as:

All international transactions on Clients Impacted by Cyber Breach list or Cards List Import 1 are declined.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Clients Impacted by Cyber Breach** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select the **Card List Import 1** list from the drop-down options.

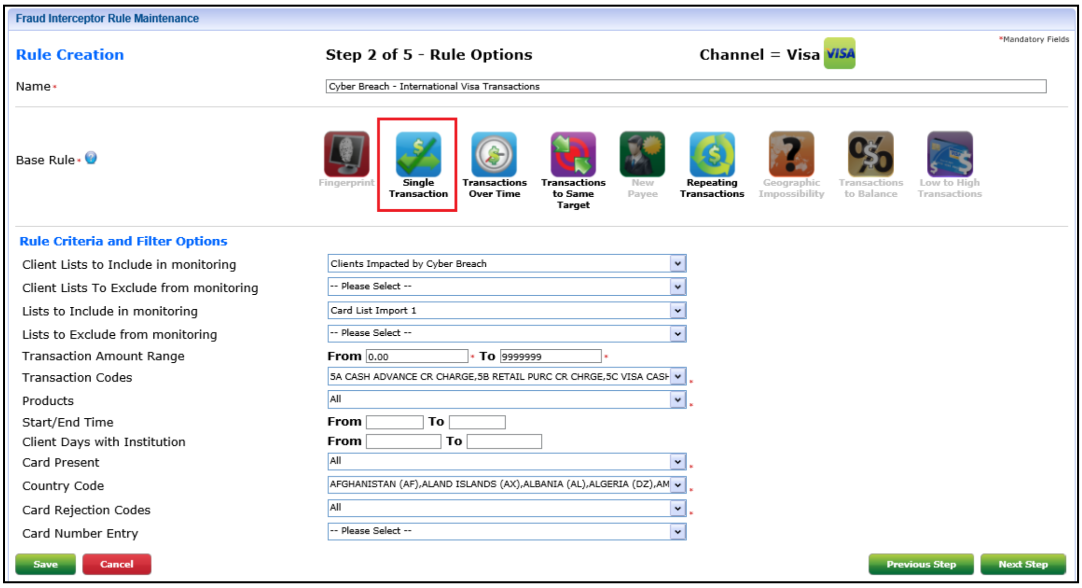
Step 2d For the **Transaction Amount Range** fields, enter **From** '0.00' **To** '9999999'.

Step 2e Select the appropriate **Transaction Codes** from the drop-down list.

Step 2f Select 'All' for the mandatory **Products**, **Card Present** and the **Card Rejection Codes** fields.

Step 2g Select all countries *other than your own*.

The easiest way to do this is to select the 'All' option from the drop-down list and then deselect your own country.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Visa**

Name*	Cyber Breach - International Visa Transactions
Base Rule*	Single Transaction

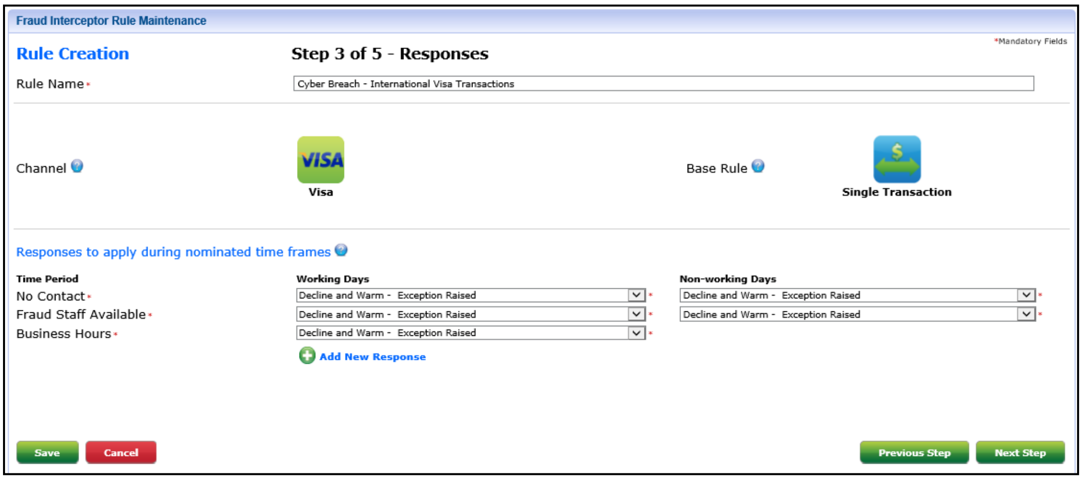
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Clients Impacted by Cyber Breach
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Card List Import 1
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	**From** 0.00 * **To** 9999999 *
Transaction Codes	5A CASH ADVANCE CR CHARGE,5B RETAIL PURC CR CHRGE,5C VISA CASH *
Products	All *
Start/End Time	**From** **To**
Client Days with Institution	**From** **To**
Card Present	All *
Country Code	AFGHANISTAN (AF),ALAND ISLANDS (AX),ALBANIA (AL),ALGERIA (DZ),AM *
Card Rejection Codes	All *
Card Number Entry	-- Please Select --

Step 2h Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following same Response from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation **Step 3 of 5 - Responses** *Mandatory Fields

Rule Name* Cyber Breach - International Visa Transactions

Channel: Visa

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Decline and Warm - Exception Raised *	Decline and Warm - Exception Raised *
Fraud Staff Available*	Decline and Warm - Exception Raised *	Decline and Warm - Exception Raised *
Business Hours*	Decline and Warm - Exception Raised *	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

Other scenarios

Personal details stolen and assumed social engineering to get payment details.

Other types of breaches may be personal data shared that enables fraudsters to use other means to target funds, like social engineering, phone porting if contact details are shared, etc.

Looking at the Fraud Interceptor layered approach for these scenarios:

- **Layer 1** – Protections for self-service channels
- **Layer 2** – Protections at the operator level so staff are able to protect customer data and not share data where the fraudster uses social engineering to change passwords to get access.
- **Layer 3** – Detect and prevent funds from leaving the organisation using your fraud rules and responses.

Lists set up for this example:

- **Cyberbreach List Clients Impacted** – manual list, go through expiry and source
- **Compromised Card List** – import from .csv simple list of card numbers

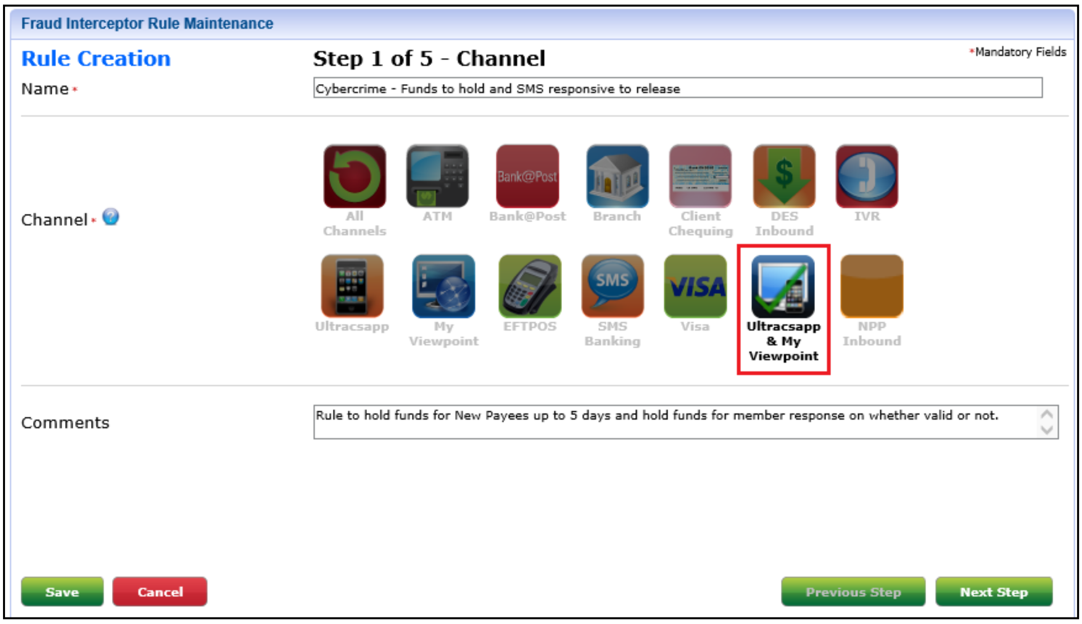
See details above for how to set up lists.

New payee, hold funds rule

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cybercrime - Funds to hold and SMS responsive to release' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Ultracsapp & My Viewpoint** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name*: Cybercrime - Funds to hold and SMS responsive to release

Channel*: Ultracsapp & My Viewpoint

Comments: Rule to hold funds for New Payees up to 5 days and hold funds for member response on whether valid or not.

Step 1d Type a descriptive entry into the **Comments** field, such as:

Rule to hold funds for New Payees up to five days and hold funds for member response on whether valid or not.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** and **New Payee** icons.

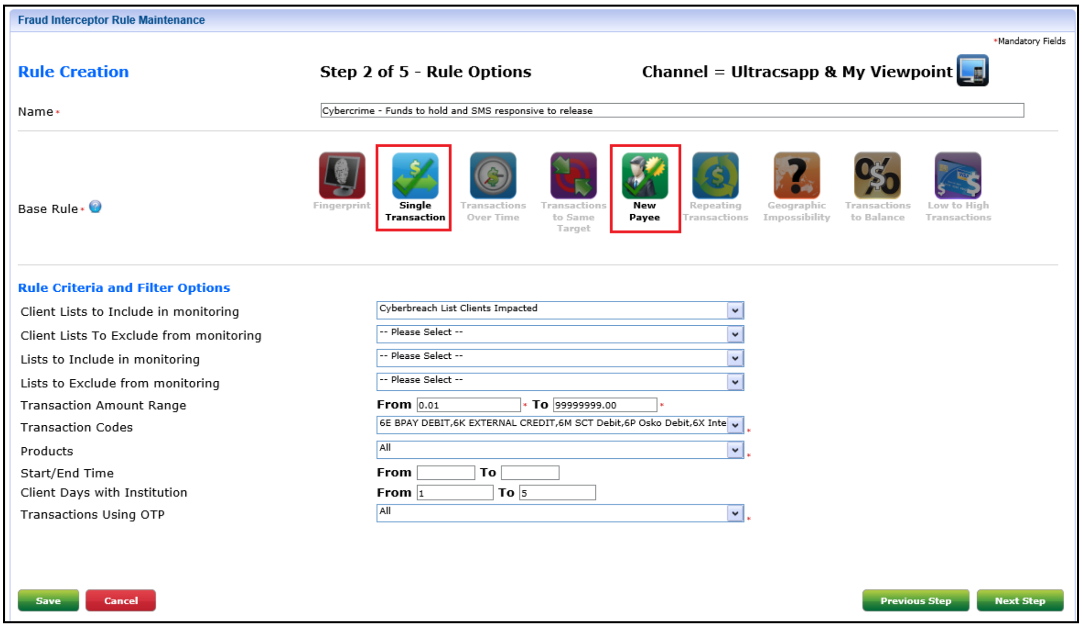
Step 2b For the **Client Lists to Include in monitoring** field, select the **Cyberbreach List Clients Impacted** list from the drop-down options.

Step 2c For the **Transaction Amount Range** fields, enter **From** '0.01' **To** '99999999.00'.

Step 2d Select the appropriate **Transaction Codes** from the drop-down list.

Step 2e Select 'All' for the mandatory **Products** and the **Transactions Using OTP** fields.

Step 2f For the **Client Days with Institution** enter a range of **From** 1 **To** 5 days.


Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation Step 2 of 5 - Rule Options Channel = Ultracsapp & My Viewpoint

Name* Cybercrime - Funds to hold and SMS responsive to release

Base Rule*

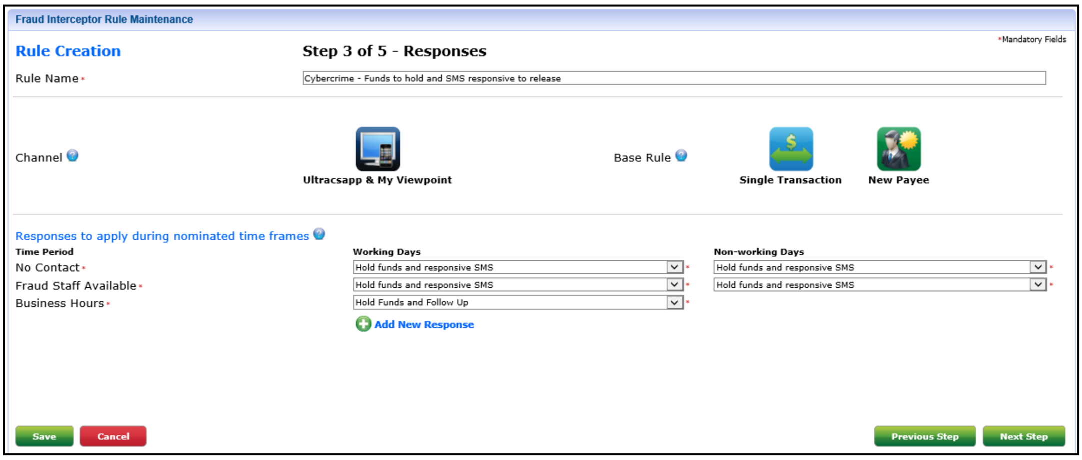
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Cyberbreach List Clients Impacted
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	**From** 0.01 * **To** 99999999.00 *
Transaction Codes	6E BPAY DEBIT,6K EXTERNAL CREDIT,6M SCT Debit,6P Osko Debit,6X Inte *
Products	All *
Start/End Time	**From** **To**
Client Days with Institution	**From** 1 **To** 5
Transactions Using OTP	All *

Step 2g Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following Responses from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation — Step 3 of 5 - Responses

*Mandatory Fields

Rule Name*: Cybercrime - Funds to hold and SMS responsive to release

Channel: Ultracsapp & My Viewpoint

Base Rule: Single Transaction, New Payee

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Hold funds and responsive SMS	Hold funds and responsive SMS
Fraud Staff Available*	Hold funds and responsive SMS	Hold funds and responsive SMS
Business Hours*	Hold Funds and Follow Up	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

Self-service transactions over $500

This rule is designed to capture any transactions made via the self-service channels that are over $500 and not New Payees and allow the member to validate the transactions using SMS Responsive.

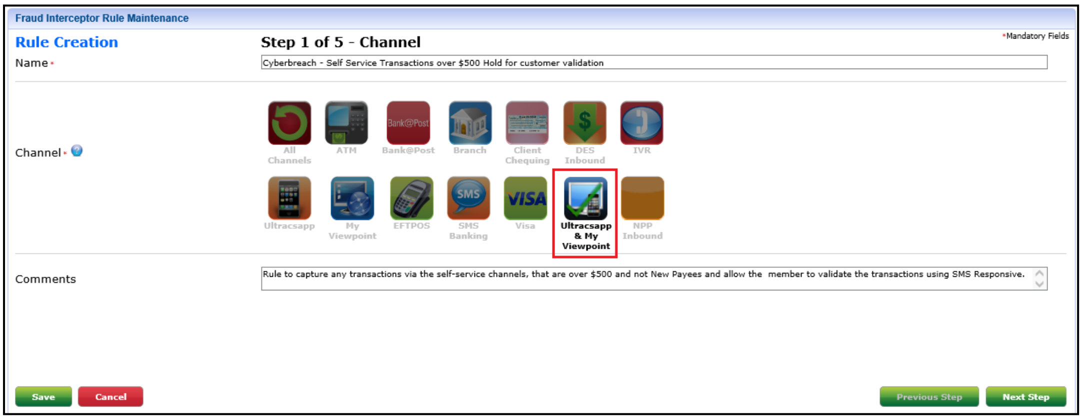
To use the SMS Responsive functionality, a template needs to be set up.

See below for an example of page to be used to define the template.

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Cyberbreach - Self Service Transactions over $500 Hold for customer validation' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Ultracsapp & My Viewpoint** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name* Cyberbreach - Self Service Transactions over $500 Hold for customer validation

Channel*

Comments Rule to capture any transactions via the self-service channels, that are over $500 and not New Payees and allow the member to validate the transactions using SMS Responsive.

Step 1d Type a descriptive entry into the **Comments** field, such as:

Rule to capture any transactions via the self-service channels, that are over $500 and not New Payees and allow the member to validate the transactions using SMS Responsive.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

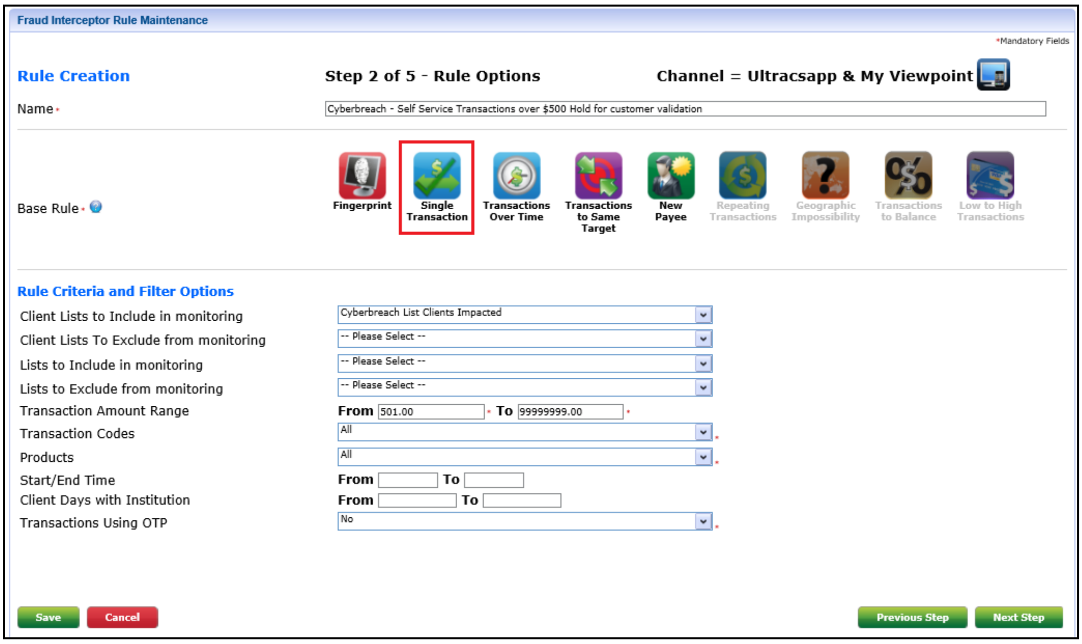
Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Cyberbreach List Clients Impacted** list from the drop-down options.

Step 2c For the **Transaction Amount Range** fields, enter **From** '501.00' **To** '99999999.00'.

Step 2d Select 'All' from the drop-down options for the mandatory **Transaction Codes** and **Products** fields.

Step 2e Select 'No' from the drop-down options for the mandatory **Transactions Using OTP** field.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Ultracsapp & My Viewpoint**

Name* Cyberbreach - Self Service Transactions over $500 Hold for customer validation

Base Rule*

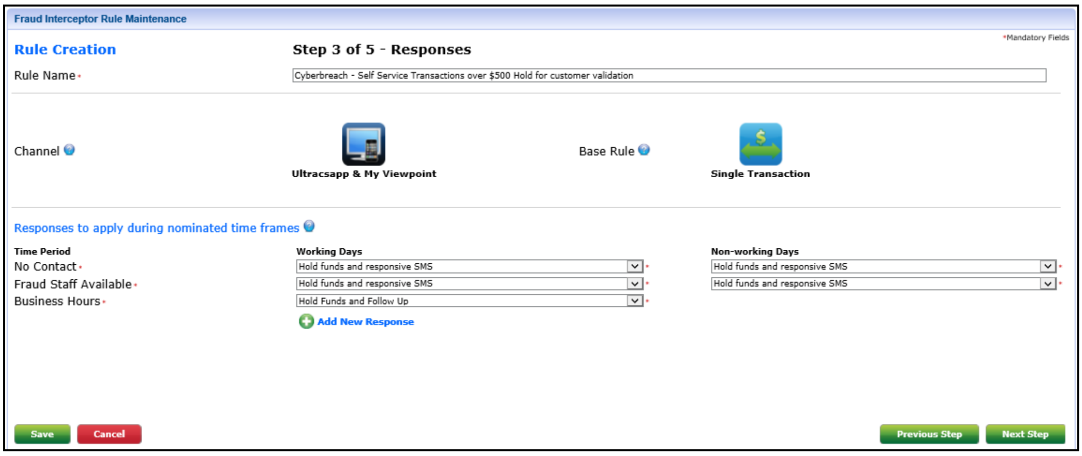
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Cyberbreach List Clients Impacted
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	**From** 501.00 * **To** 99999999.00 *
Transaction Codes	All *
Products	All *
Start/End Time	**From** **To**
Client Days with Institution	**From** **To**
Transactions Using OTP	No *

Step 2f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following Responses from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 3 of 5 - Responses**

Rule Name* Cyberbreach - Self Service Transactions over $500 Hold for customer validation

Channel: Ultracsapp & My Viewpoint

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Hold funds and responsive SMS	Hold funds and responsive SMS
Fraud Staff Available*	Hold funds and responsive SMS	Hold funds and responsive SMS
Business Hours*	Hold Funds and Follow Up	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

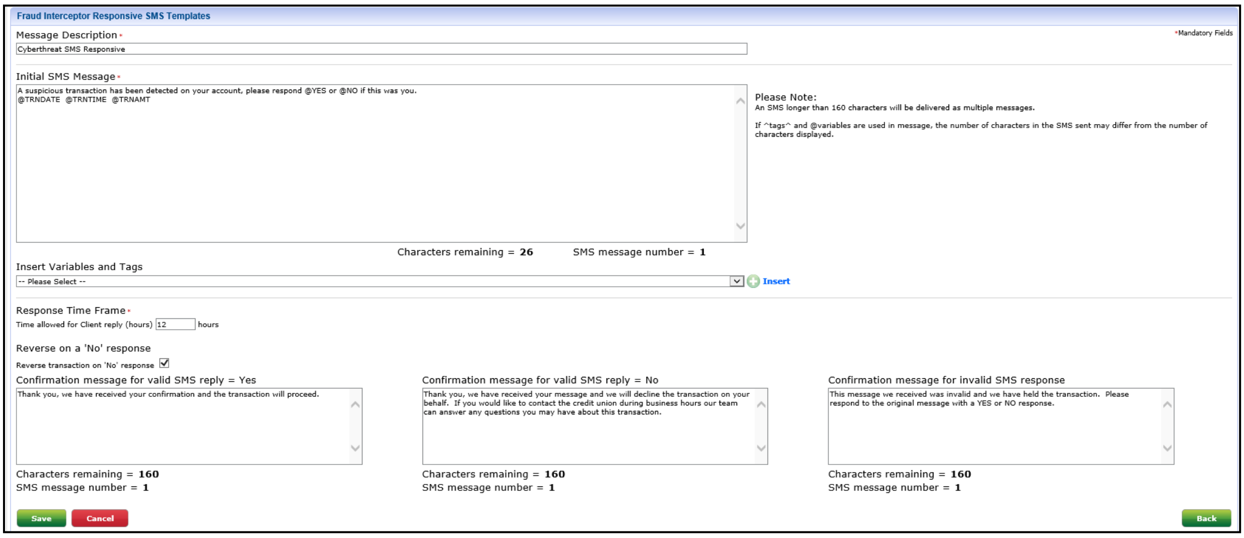
An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

Fraud Interceptor Responsive SMS Templates

Below is an example of the page used to facilitate the use of the SMS Responsive feature.

Refer to the **Responsive SMS Templates** topic in the *Fraud Interceptor User Manual* for full details of how to complete this page.



Fraud Interceptor Responsive SMS Templates

*Mandatory Fields

Message Description*

Cyberthreat SMS Responsive

Initial SMS Message*

A suspicious transaction has been detected on your account, please respond @YES or @NO if this was you.
@TRNDATE @TRNTIME @TRNAMT

Please Note:
An SMS longer than 160 characters will be delivered as multiple messages.

If ^tags^ and @variables are used in message, the number of characters in the SMS sent may differ from the number of characters displayed.

Characters remaining = **26** SMS message number = **1**

Insert Variables and Tags

-- Please Select --

Response Time Frame*

Time allowed for Client reply (hours) 12 hours

Reverse on a 'No' response

Reverse transaction on 'No' response ☑

Confirmation message for valid SMS reply = Yes

Thank you, we have received your confirmation and the transaction will proceed.

Characters remaining = **160**
SMS message number = **1**

Confirmation message for valid SMS reply = No

Thank you, we have received your message and we will decline the transaction on your behalf. If you would like to contact the credit union during business hours our team can answer any questions you may have about this transaction.

Characters remaining = **160**
SMS message number = **1**

Confirmation message for invalid SMS response

This message we received was invalid and we have held the transaction. Please respond to the original message with a YES or NO response.

Characters remaining = **160**
SMS message number = **1**

Crypto Currency

With interest and awareness of crypto-currencies growing, more and more people - and their financial institutions - are at risk of falling victim to crypto-currency scams.

Crypto-currencies can be held anonymously and transferred worldwide quickly, making it the preferred payment method for scammers. In the twelve months to August 2024, the Australian Federal Police reported that Australians lost $180 million worth of crypto-currency in investment scams.

The targets can be investment schemes that are too good to be true or romance scams and uses social engineering to convince consumers to part with their money. Once the funds are sent to the “broker” then the investment disappears.

The key to tackling this is to have lists specific for known fraudulent companies and known Merchant Category Codes (MCC) as well as other payment methods.

Financial institutions already running Ultracs Fraud Interceptor have shared some of their experiences / guidelines:

- A minimum level of losses seems to occur as Remote Access Scams using Osko payments. Analysis of these scams show threat actors have shifted their strategy to obtain card details as well and then proceed to debit cards with the merchants being crypto currency providers. Key examples of this relates to Ria Financial Services, World Remit, Remitly and many others.
- Threat actors are monetising compromised payment credentials in similar ways as other Card Not Present (CNP) methods.
- Pay particular attention to transactions where the Merchant Category Code is 4829 – Wires, Money Orders. Also, a number of merchants use 'unusual' MCCs, for example 6051 – Quasi Cash.
- Rules should cover *all* payment channels and their respective identifiers.
- Set up the following lists. Monitoring rules and collaboration with peers are valuable tools to assist with this.
  - **Merchant List** – A list with names of merchants that are known as fraudulent merchants.
  - **MCC List** – Codes that it has been found that fraud happens through in crypto currency transactions.
  - **BSB List** – Blacklist known BSBs / accounts used by crypto brokerages but have to keep an eye out for new ones popping up.
  - **BPAY Whitelist** – Approved BPAY Billers
  - **BPAY Non-Whitelist** – Non-whitelisted BPAY Billers generally include crypto brokerages, overseas funds transfer providers and credit cards.

Refer to the **Setting up lists** topic in the Cyber Breaches section of this manual for further information.

Below is an outline of the process for setting up Rules specifically to minimise scams related to crypto-currencies.

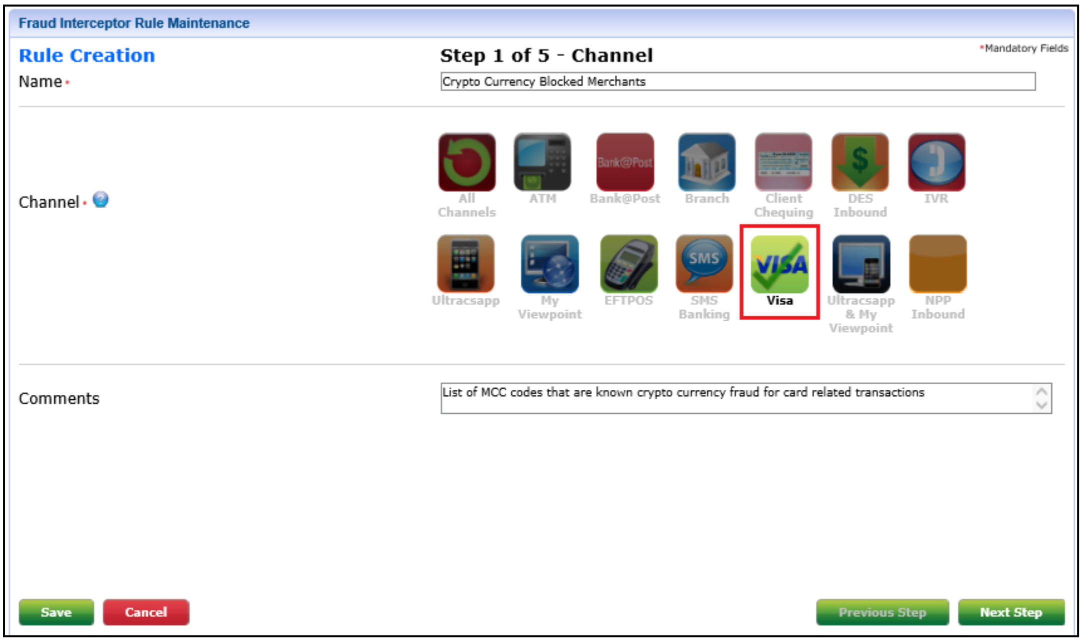
Refer to the *Fraud Interceptor User Manual* for full details of the five steps involved to set up each Rule.

Blocked Merchant Category Codes

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Crypto Currency Blocked Merchants' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name*: Crypto Currency Blocked Merchants

Channel*: Visa

Comments: List of MCC codes that are known crypto currency fraud for card related transactions

Step 1d Type a descriptive entry into the **Comments** field, such as:

List of MCCs that are known crypto currency fraud for card related transactions.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

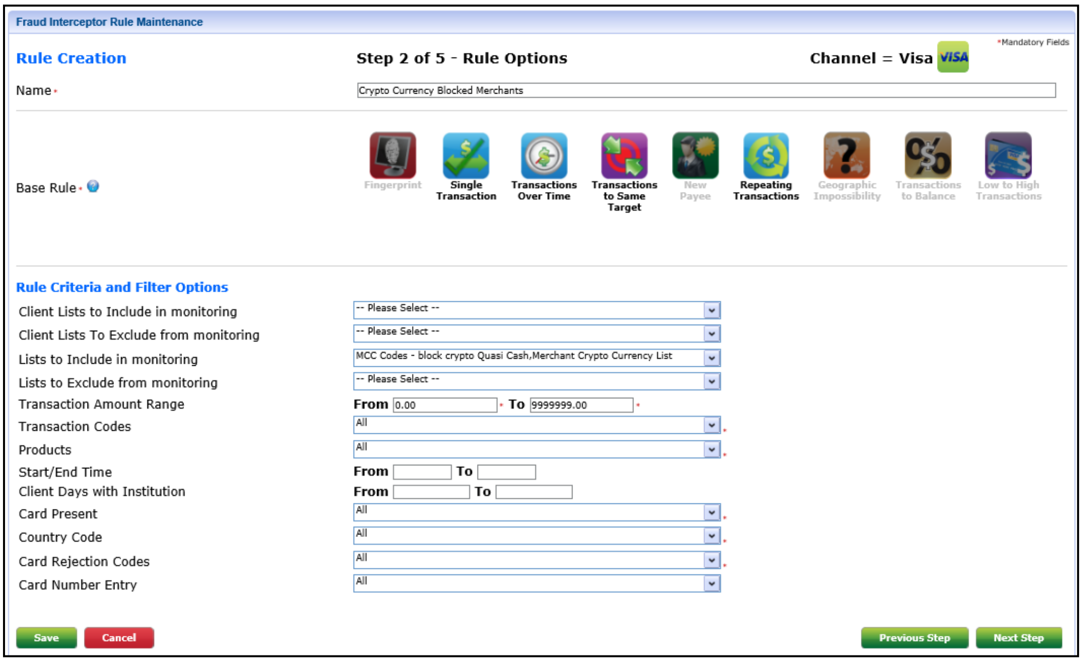
Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Lists to Include in monitoring** field, select from the drop-down options, all the related lists you have prepared. For example, MCC List, Merchant Crypto Currency List.

Step 2c For the **Transaction Amount Range** fields, enter **From** '0.01' **To** '9999999.00'.

Step 2d Select 'All' for the mandatory **Transaction Codes**, **Products**, **Card Present**, **Country Code**, **Card Reject Codes** and (if applicable) **Card Number Entry** fields.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 2 of 5 - Rule Options

Channel = Visa

*Mandatory Fields

Name* Crypto Currency Blocked Merchants

Base Rule*

Rule Criteria and Filter Options

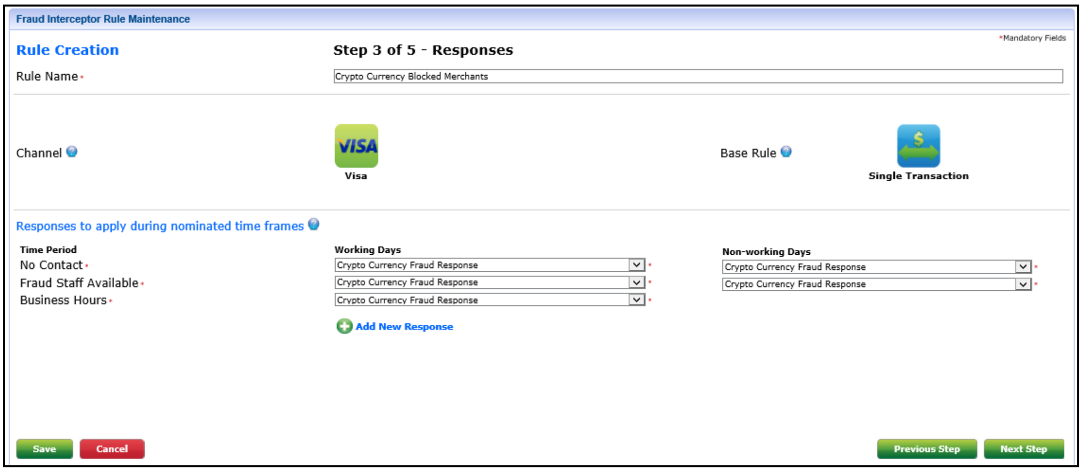
Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	MCC Codes - block crypto Quasi Cash,Merchant Crypto Currency List
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	**From** 0.00 * **To** 9999999.00 *
Transaction Codes	All *
Products	All *
Start/End Time	**From** **To**
Client Days with Institution	**From** **To**
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	All

Step 2e

Step 2f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following same Response from the drop-down lists of options for each of the five fields:



Rule Creation

Step 3 of 5 - Responses

*Mandatory Fields

Rule Name* Crypto Currency Blocked Merchants

Channel: Visa

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Crypto Currency Fraud Response*	Crypto Currency Fraud Response*
Fraud Staff Available*	Crypto Currency Fraud Response*	Crypto Currency Fraud Response*
Business Hours*	Crypto Currency Fraud Response*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

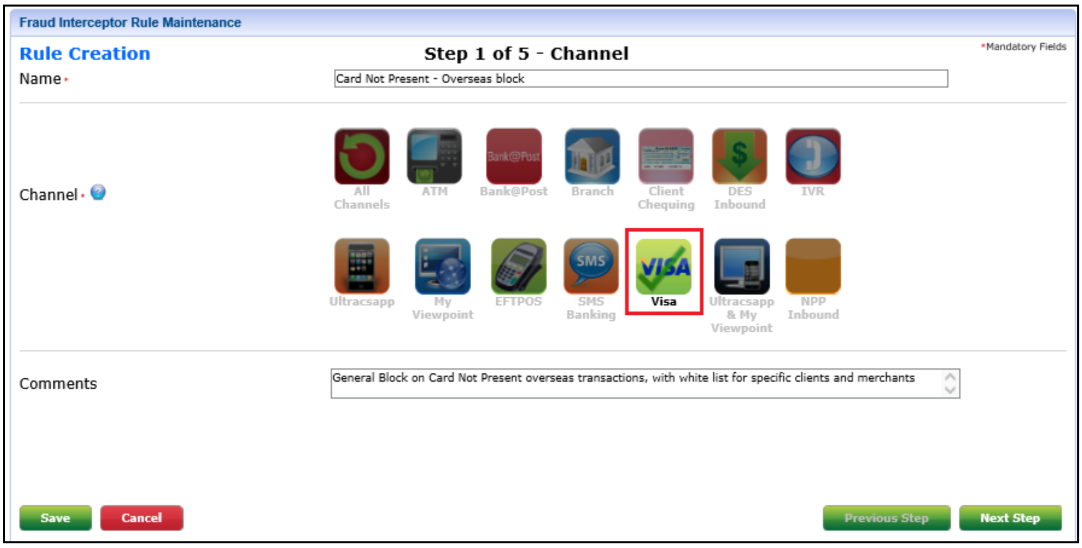
If required, click the **Previous Step** button go back to earlier steps.

Card Not Present - Overseas Block

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Card Not Present - Overseas block' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Visa** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name*: Card Not Present - Overseas block

Channel*: Visa

Comments: General Block on Card Not Present overseas transactions, with white list for specific clients and merchants

Step 1d Type a descriptive entry into the **Comments** field, such as:

General Block on Card Not Present overseas transactions, with white list for specific clients and merchants

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

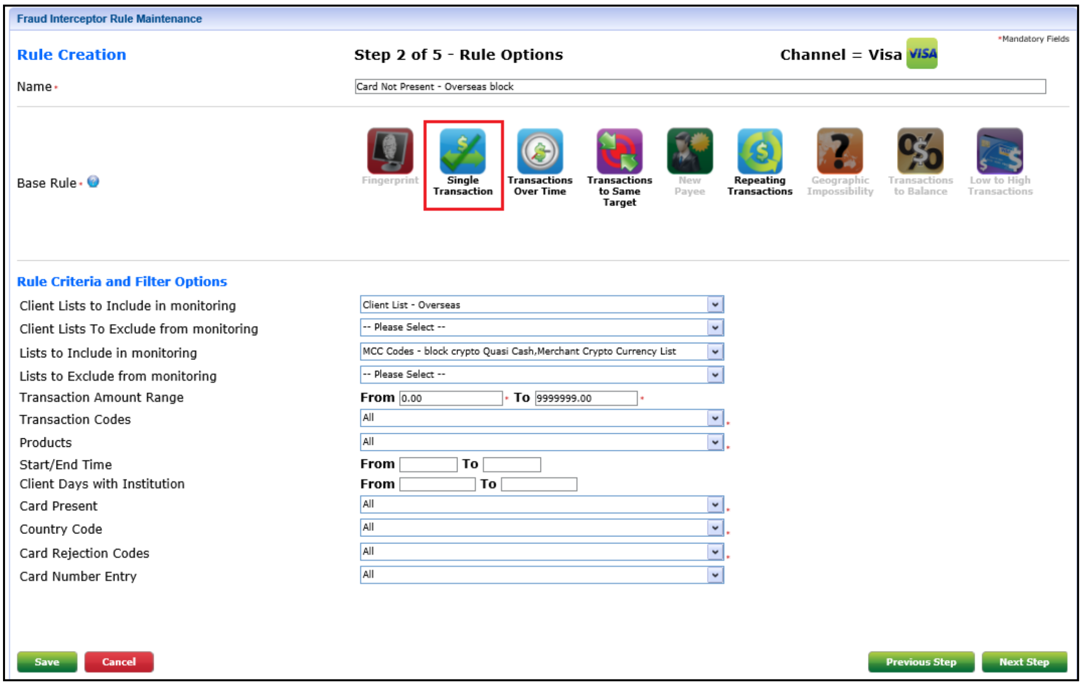
Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b For the **Client Lists to Include in monitoring** field, select the **Client List - Overseas** list from the drop-down options.

Step 2c For the **Lists to Include in monitoring** field, select from the drop-down options, all the related lists you have prepared. For example, MCC Codes - block crypto Quasi Cash, Merchant Crypto Currency List.

Step 2d Select 'All' for the mandatory **Transaction Codes**, **Products**, **Card Present**, **Country Code**, **Card Rejection Codes** and (if applicable) **Card Number Entry** fields.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation   Step 2 of 5 - Rule Options   Channel = Visa

Name*	Card Not Present - Overseas block
Base Rule*	Single Transaction

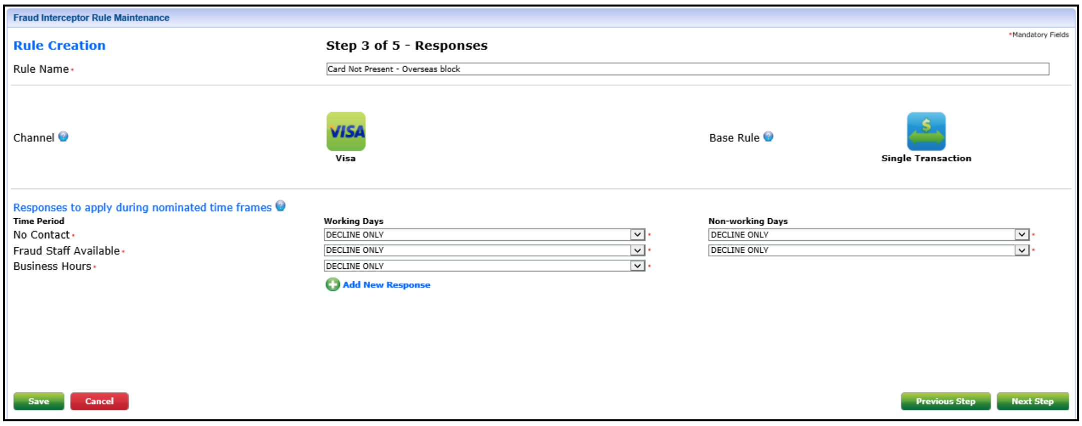
Rule Criteria and Filter Options

Client Lists to Include in monitoring	Client List - Overseas
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	MCC Codes - block crypto Quasi Cash,Merchant Crypto Currency List
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 0.00 * To 9999999.00 *
Transaction Codes	All *
Products	All *
Start/End Time	From To
Client Days with Institution	From To
Card Present	All *
Country Code	All *
Card Rejection Codes	All *
Card Number Entry	All

Step 2e Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the 'DECLINE ONLY' Response from the drop-down lists of options for all of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation **Step 3 of 5 - Responses** *Mandatory Fields

Rule Name* Card Not Present - Overseas block

Channel: Visa

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	DECLINE ONLY	DECLINE ONLY
Fraud Staff Available*	DECLINE ONLY	DECLINE ONLY
Business Hours*	DECLINE ONLY	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

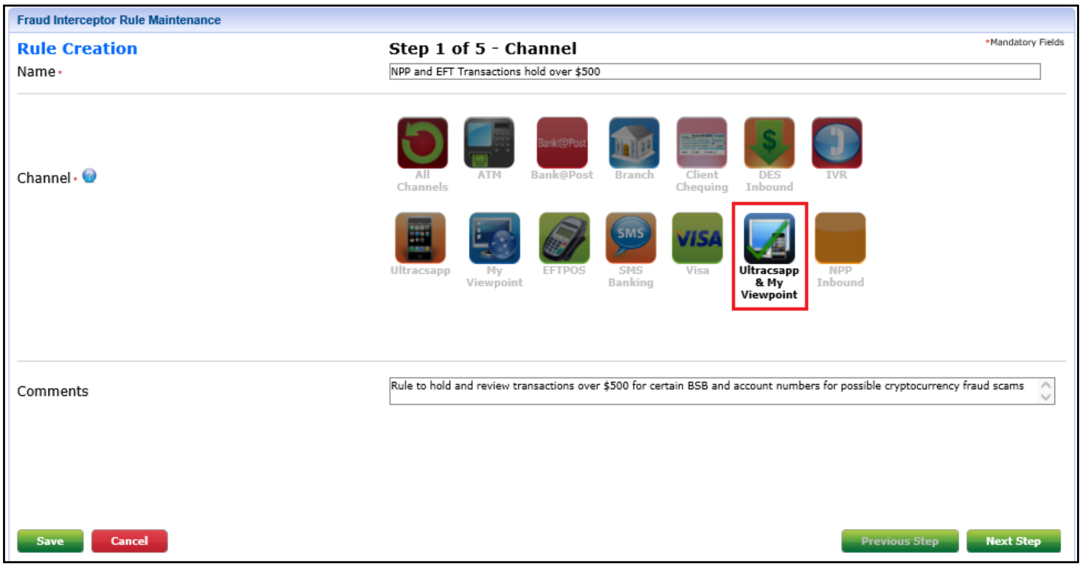
If required, click the **Previous Step** button go back to earlier steps.

NPP and EFT Transactions over $500 - Hold and Review

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'NPP and EFT Transactions hold over $500' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **Ultracsapp & My Viewpoint** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name* NPP and EFT Transactions hold over $500

Channel*

Comments: Rule to hold and review transactions over $500 for certain BSB and account numbers for possible cryptocurrency fraud scams

Step 1d Type a descriptive entry into the **Comments** field, such as:

Rule to hold and review transactions over $500 for certain BSB and account numbers for possible cryptocurrency fraud scams.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

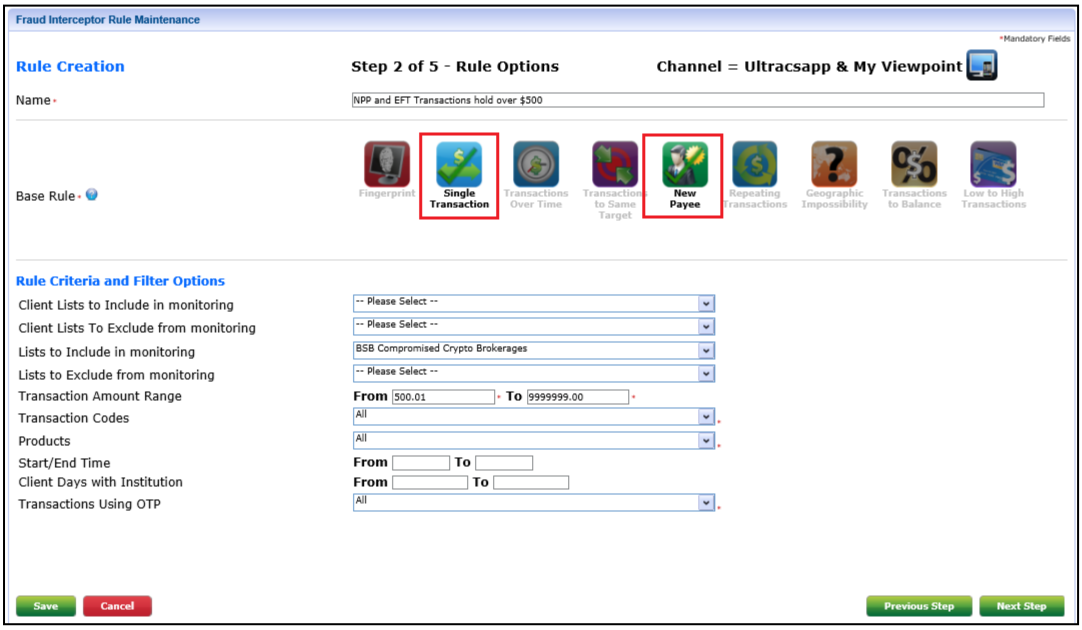
Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** and the **New Payee** icons.

Step 2b For the **Lists to Include in monitoring** field, select the **BSB Compromised Crytpo Brokerages** list from the drop-down options.

Step 2c For the **Transaction Amount Range** fields, enter **From** '0.00' **To** '9999999.00'.

Step 2d Select 'All' for the mandatory **Transaction Codes**, **Products**, and **Transactions Using OTP** fields.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 2 of 5 - Rule Options

Channel = Ultracsapp & My Viewpoint

Name*: NPP and EFT Transactions hold over $500

Base Rule*: Single Transaction, New Payee

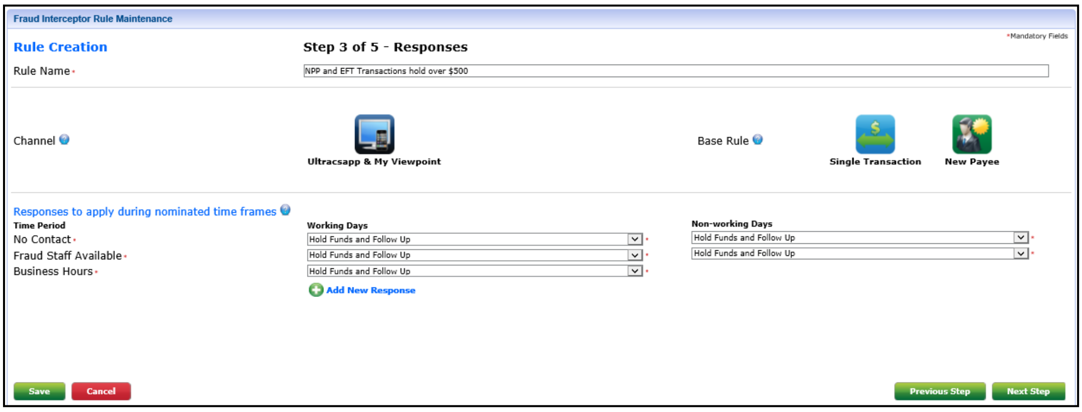
Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	BSB Compromised Crypto Brokerages
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 500.01 * To 9999999.00 *
Transaction Codes	All *
Products	All *
Start/End Time	From To
Client Days with Institution	From To
Transactions Using OTP	All *

Step 2e Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the 'Hold Funds and Follow Up' Response from the drop-down lists of options for all of the five fields:



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 3 of 5 - Responses

Rule Name*: NPP and EFT Transactions hold over $500

Channel: Ultracsapp & My Viewpoint

Base Rule: Single Transaction, New Payee

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Hold Funds and Follow Up	Hold Funds and Follow Up
Fraud Staff Available*	Hold Funds and Follow Up	Hold Funds and Follow Up
Business Hours*	Hold Funds and Follow Up	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

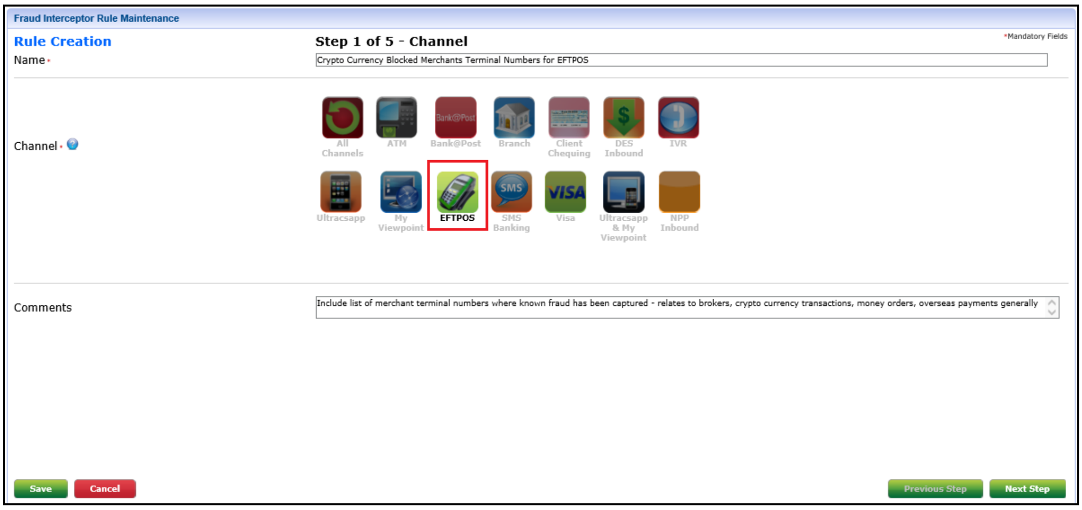
If required, click the **Previous Step** button go back to earlier steps.

Blocking EFTPOS Terminals of Known Crypto Currency Merchants

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'Crypto Currency Blocked Merchants Terminal Numbers for EFTPOS' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **EFTPOS** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name*: Crypto Currency Blocked Merchants Terminal Numbers for EFTPOS

Channel*: EFTPOS

Comments: Include list of merchant terminal numbers where known fraud has been captured - relates to brokers, crypto currency transactions, money orders, overseas payments generally

Step 1d Type a descriptive entry into the **Comments** field, such as:

Include list of merchant terminal numbers where known fraud has been captured - relates to brokers, crypto currency transactions, money orders, overseas payments generally

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

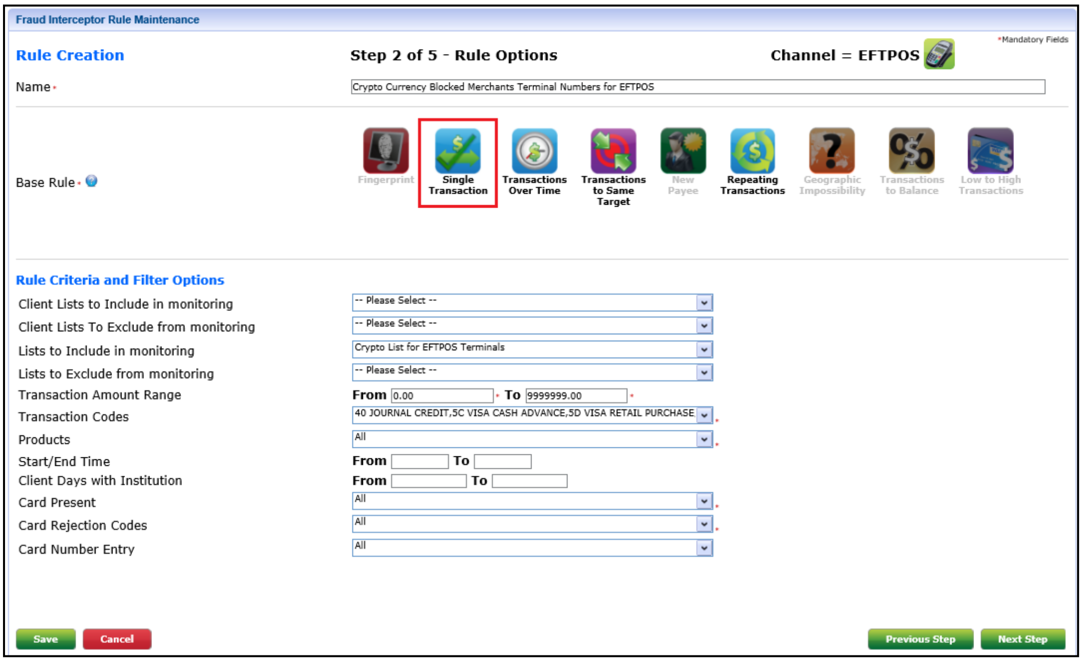
Step 2b For the **Lists to Include in monitoring** field, select **Crypto List for EFTPOS Terminals** from the drop-down options.

Step 2c For the **Transaction Amount Range** fields, enter **From** '0.00' **To** '9999999.00'.

Step 2d Select the appropriate **Transaction Codes** from the drop-down list.

Step 2e

Select 'All' for the **Products**, **Card Present**, **Card Rejection Codes** and (if applicable) **Card Number Entry** fields.



Fraud Interceptor Rule Maintenance

Rule Creation — Step 2 of 5 - Rule Options — Channel = EFTPOS

*Mandatory Fields

Name*: Crypto Currency Blocked Merchants Terminal Numbers for EFTPOS

Base Rule*:

Rule Criteria and Filter Options

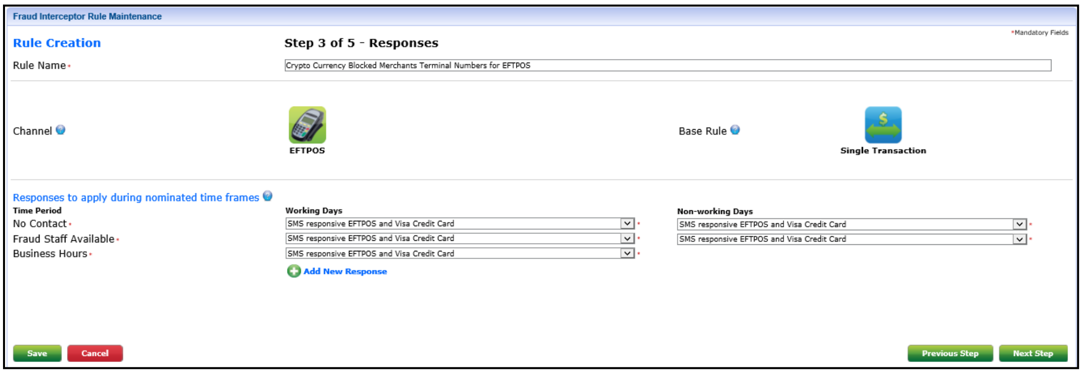
Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	Crypto List for EFTPOS Terminals
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 0.00* To 9999999.00*
Transaction Codes	40 JOURNAL CREDIT,5C VISA CASH ADVANCE,5D VISA RETAIL PURCHASE*
Products	All*
Start/End Time	From To
Client Days with Institution	From To
Card Present	All*
Card Rejection Codes	All*
Card Number Entry	All

Step 2f

Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the 'SMS responsive EFTPOS and Visa Credit Card' Response from the drop-down lists of options for all of the five fields:



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation — Step 3 of 5 - Responses

Rule Name* Crypto Currency Blocked Merchants Terminal Numbers for EFTPOS

Channel: EFTPOS

Base Rule: Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	SMS responsive EFTPOS and Visa Credit Card*	SMS responsive EFTPOS and Visa Credit Card*
Fraud Staff Available*	SMS responsive EFTPOS and Visa Credit Card*	SMS responsive EFTPOS and Visa Credit Card*
Business Hours*	SMS responsive EFTPOS and Visa Credit Card*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

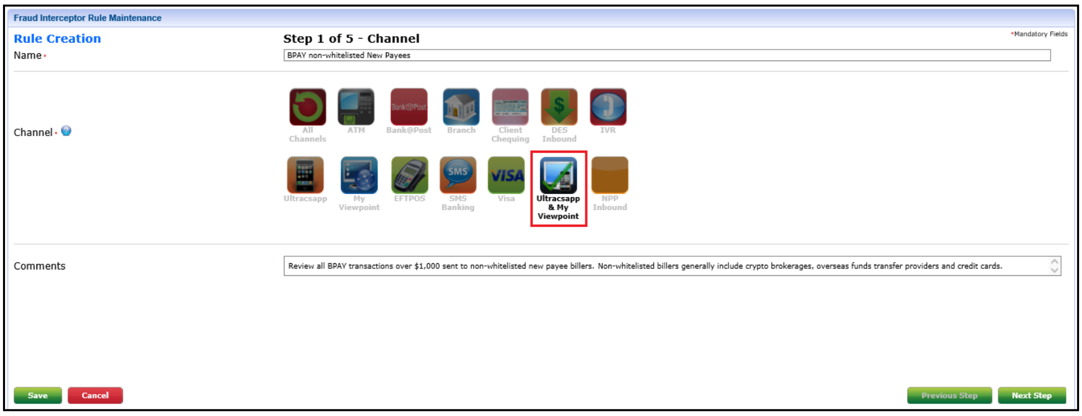
If required, click the **Previous Step** button go back to earlier steps.

New BPAY Payees - non-whitelisted

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.

Step 1b Enter 'BPAY non-whitelisted New Payees' (or a similar description) in the **Name** field.

Step 1c For the **Channel**, click on the **EFTPOS** icon.



Fraud Interceptor Rule Maintenance

Rule Creation

Step 1 of 5 - Channel

*Mandatory Fields

Name*: BPAY non-whitelisted New Payees

Channel*

Comments: Review all BPAY transactions over $1,000 sent to non-whitelisted new payee billers. Non-whitelisted billers generally include crypto brokerages, overseas funds transfer providers and credit cards.

Step 1d Type a descriptive entry into the **Comments** field, such as:

Review all BPAY transactions over $1,000 sent to non-whitelisted new payee billers. Non-whitelisted billers generally include crypto brokerages, overseas funds transfer providers and credit cards.

Step 1e Click **Save**.

Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

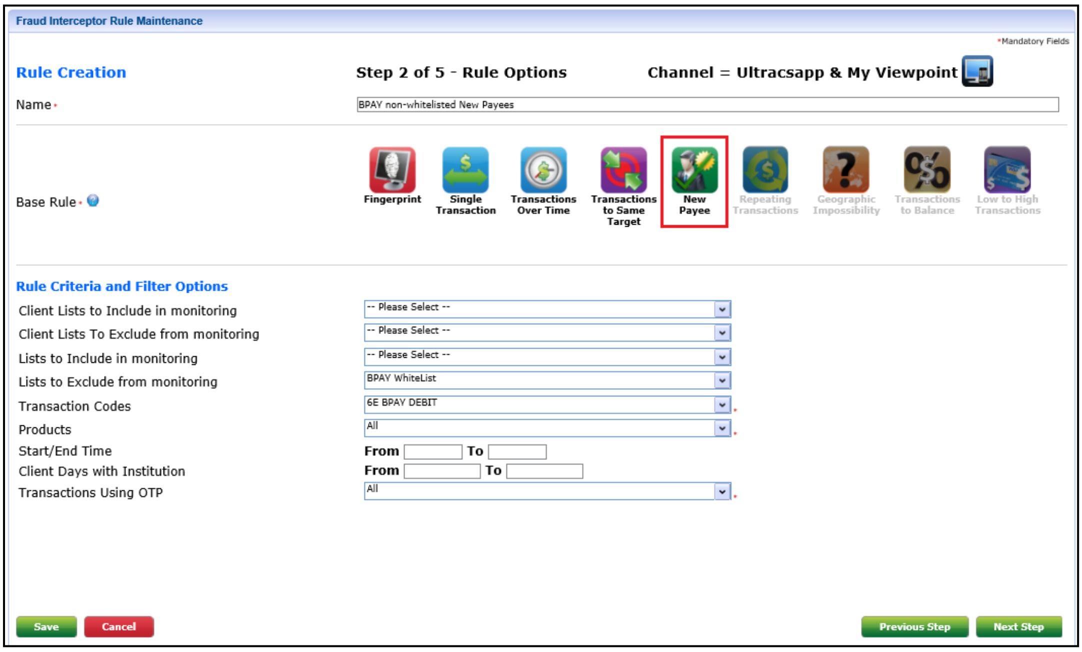
Step 2a For the **Base Rule**, click on the **New Payee** icon.

Step 2b For the **Lists to Exclude from monitoring** field, select **BPAY WhiteList** from the drop-down options.

Step 2c Select the appropriate **Transaction Codes** from the drop-down list.

Step 2d

Select 'All' for the **Products** and **Transactions Using OTP** fields.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = Ultracsapp & My Viewpoint**

Name* BPAY non-whitelisted New Payees

Base Rule*

Rule Criteria and Filter Options

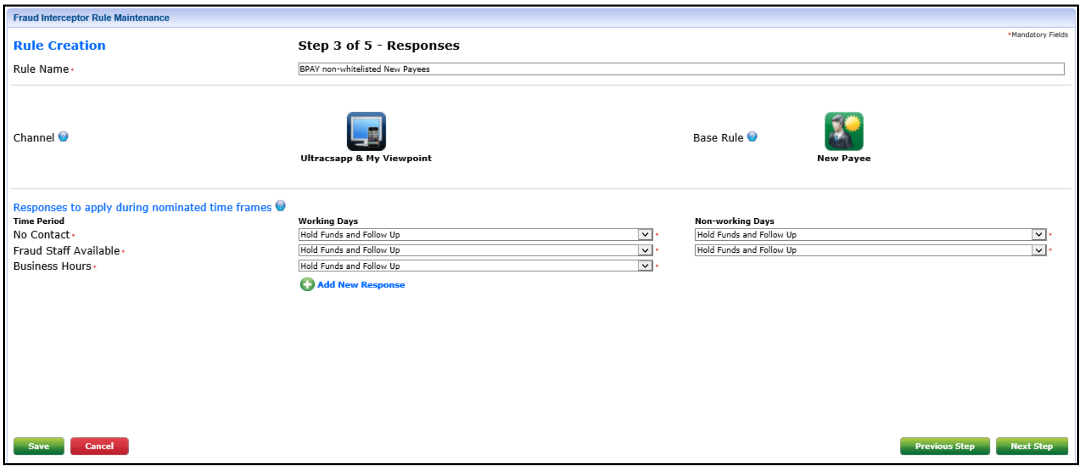
Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	BPAY WhiteList
Transaction Codes	6E BPAY DEBIT *
Products	All *
Start/End Time	**From** **To**
Client Days with Institution	**From** **To**
Transactions Using OTP	All *

Step 2e

Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the 'Hold Funds and Follow Up' Response from the drop-down lists of options for all of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation

Step 3 of 5 - Responses

*Mandatory Fields

Rule Name*	BPAY non-whitelisted New Payees
Channel	Ultracsapp & My Viewpoint
Base Rule	New Payee

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	Hold Funds and Follow Up*	Hold Funds and Follow Up*
Fraud Staff Available*	Hold Funds and Follow Up*	Hold Funds and Follow Up*
Business Hours*	Hold Funds and Follow Up*	

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

Branch Channel Rules

The following example is a scenario that may be useful for monitoring Branch transactions.

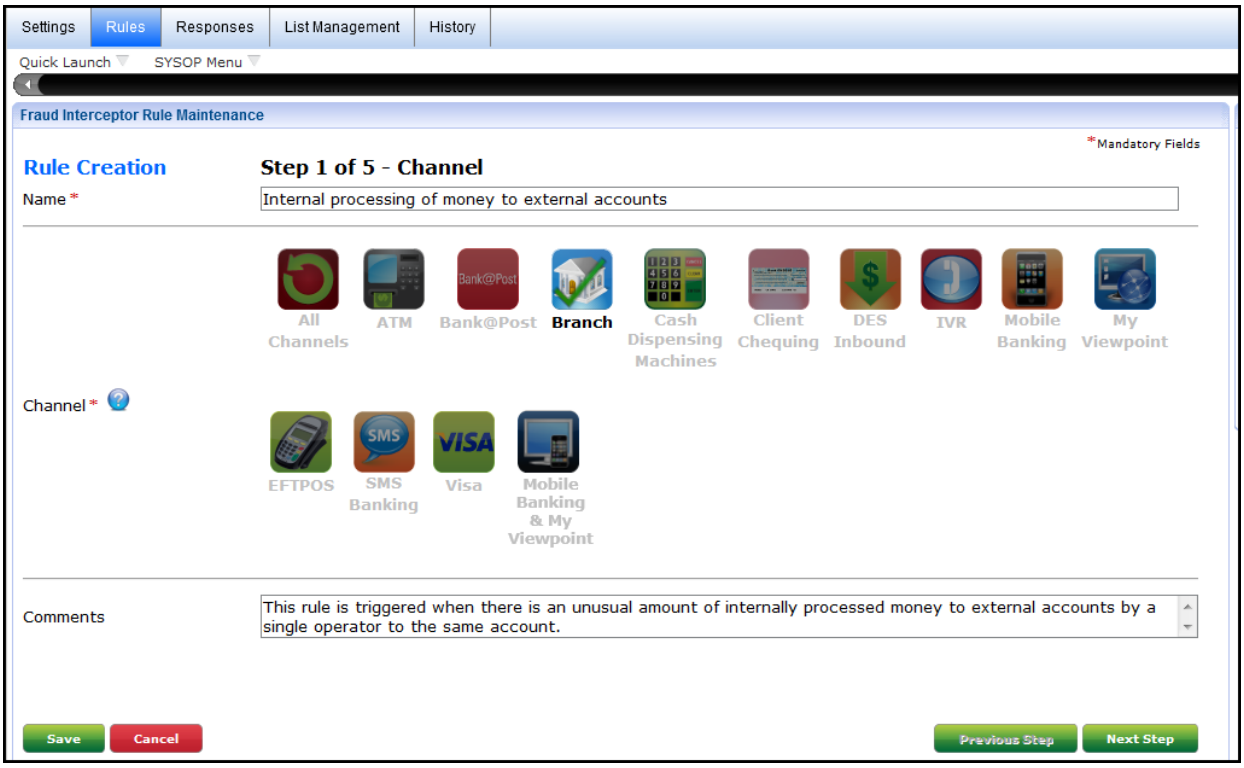
- Internal processing of money to external accounts (i.e. DES)

Internal processing of money to external accounts (i.e. DES)

This rule is designed to be triggered when there is an unusual amount of internal processing of money to external accounts by a single operator to the same account. This rule is designed around picking up multiple external credit transactions to the same account over a specified period of time.

This example targets four transactions to the same account within five days totalling $100,000 or more. You may find different criteria more suitable for your needs.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Step 1 of 5 - Channel

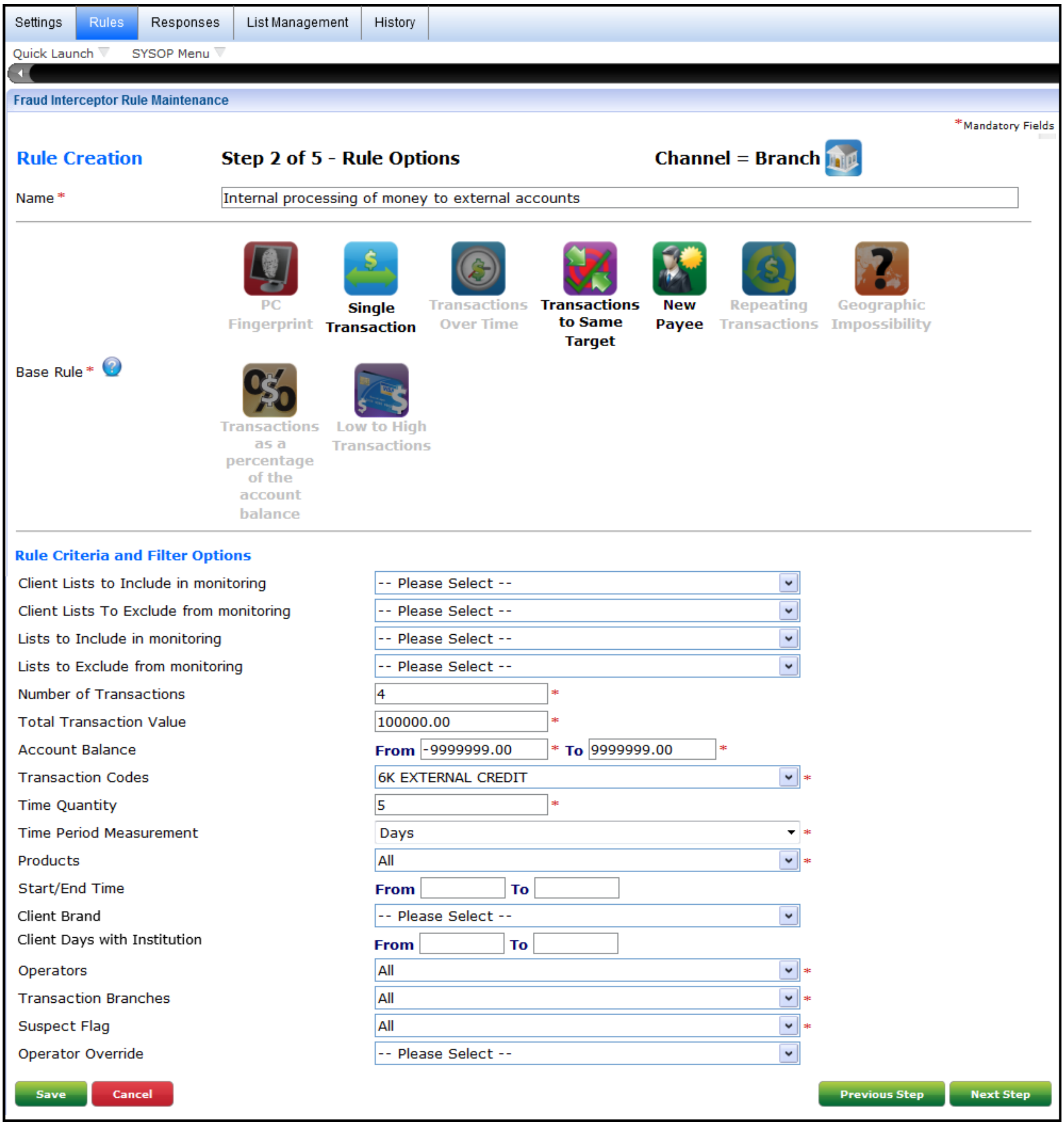
Name * Internal processing of money to external accounts

Channel * Branch

Comments This rule is triggered when there is an unusual amount of internally processed money to external accounts by a single operator to the same account.

This rule uses the Branch Channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation — **Step 2 of 5 - Rule Options** — **Channel = Branch**

Name *	Internal processing of money to external accounts
Base Rule *	Transactions to Same Target

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	4 *
Total Transaction Value	100000.00 *
Account Balance	From -9999999.00 * To 9999999.00 *
Transaction Codes	6K EXTERNAL CREDIT *
Time Quantity	5 *
Time Period Measurement	Days *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Operators	All *
Transaction Branches	All *
Suspect Flag	All *
Operator Override	-- Please Select --

This rule uses the Base Rule 'Transactions to Same Target'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	Lists have not been used with this rule as you wish to target all transactions.

Number of Transactions	The scenario is triggered when '4' transactions occur within the specified timeframe.
Total Transaction Value	This rule is triggered if the transactions total at least $100,000 so 100000.00 has been entered into this field.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate transaction codes. In this example, External Credits have been targeted.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '5' and 'Days' have been selected.
Products	'All' has been selected; however, if you only have one or two products types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Operators	Select the operators to be included in this rule. In this example, 'All' has been selected; however, you could target specific operators instead.
Transaction Branches	Select the branches from which the transactions originate to include in this rule. In this example, 'All' has been selected; however, you could target specific branches instead.
Suspect Flag	While it is unlikely that an operator targeted by this rule will flag their transactions as 'suspect', you may as well select 'All' so that no transactions that meet the other requirements are excluded.
Operator Override	This field is not mandatory and has been left blank in this example. This ensures that transactions are not excluded from the rule based on whether or not an Operator Override was used when the transaction was performed.

EFTPOS Channel Rules

This section gives step-by-step examples of how to set up a fraud rule for specific EFTPOS-related scenarios.

Least Cost Routing

Some merchants' POS terminals are set up with the Least Cost Routing option.

This means that their customers' credit card transactions may be routed through the domestic **eftpos*** network (a cheaper option for the merchant) instead of being directed via the credit card network used by Visa / Mastercard.

> * The all-lower-case 'eftpos' is a brand name of Australia's domestic debit card network, operated by Australian Payments Plus (AP+).

The option of “least cost routing” was available to some large corporations such as major supermarkets and the facility has expanded to other merchants, such as online meal ordering. This opens the door for fraudsters to compromise the channel for merchants that may not have as robust security as others.

Background

If a transaction comes through the eftpos network, there are no charge-back options for your financial institution and the transaction is forced down the line thus ensuring that the fraudster gets their money immediately.

Fraudsters can clone the magnetic strip of a card onto another card. If they then corrupt the card's chip, the terminal will fall-back to using the compromised magstrip and the merchant is then unwittingly processing the transaction through the eftpos network and there are no charge-back options.

To assist in preventing fraudulent transactions, switch providers have made some changes:

Cuscal Switch clients – Cuscal have added a **Card Entry Mode** '21', labelled in Ultracs as 'Cuscal Eftpos Fallback' allowing you to identify any transactions that have been validated as invalid and should be declined. This additional entry mode requires the Ultradata Support Services team to make an update to the table in Ultracs. Please log a Jira case as soon as possible to have this done.

Your financial institution may wish to contact Cuscal and ask them to make a change for these fall-back transactions; that could be in addition to setting it up in Fraud Interceptor.

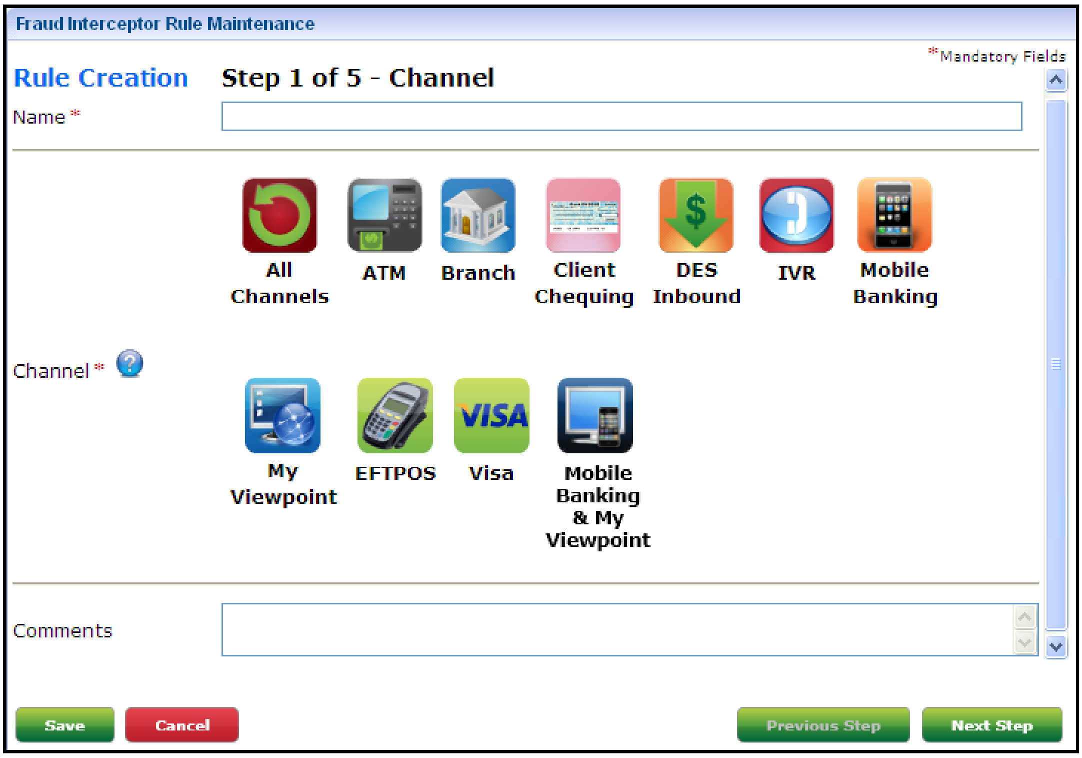
Fiserv Switch clients – Fiserv are declining at the switch and you don’t see these transactions.

Setting up the Rule

Below is an outline of the process, highlighting the key settings for Least Cost Routing transactions.

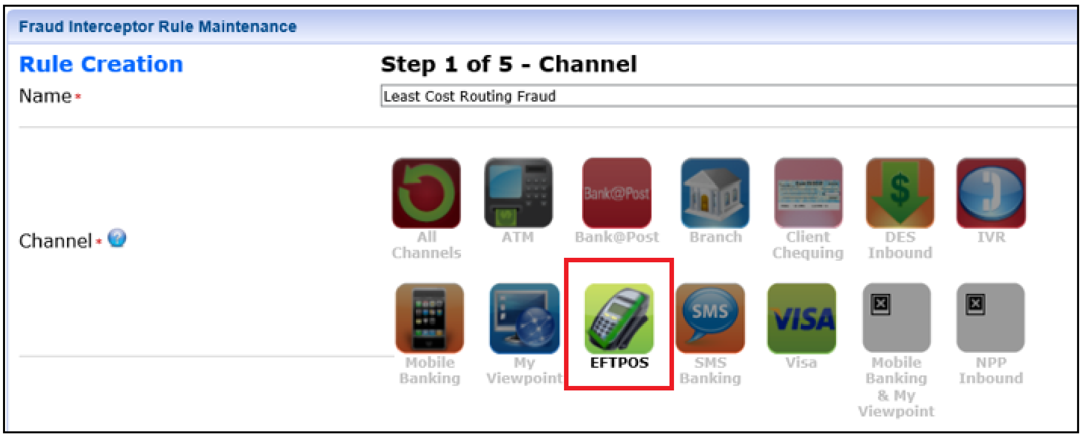
Refer to the *Fraud Interceptor User Manual* for full details of the five steps involved.

Step 1a Navigate to the **Rule Creation - Step 1 of 5 - Channel** page.



Step 1b Enter 'Least Cost Routing Fraud' in the **Name** field.

Step 1c For the **Channel**, click on the **EFTPOS** icon.



Name * Least Cost Routing Fraud

Step 1d Type a descriptive entry into the **Comments** field, such as:

This rule is designed to reject any transactions that initiated as Visa but were pushed through the EFTPOS network under the Least Cost Routing method used by the merchant.

Card Entry Mode21 *(Cuscal Eftpos Fallback) applies.*

Step 1e Click **Save**.

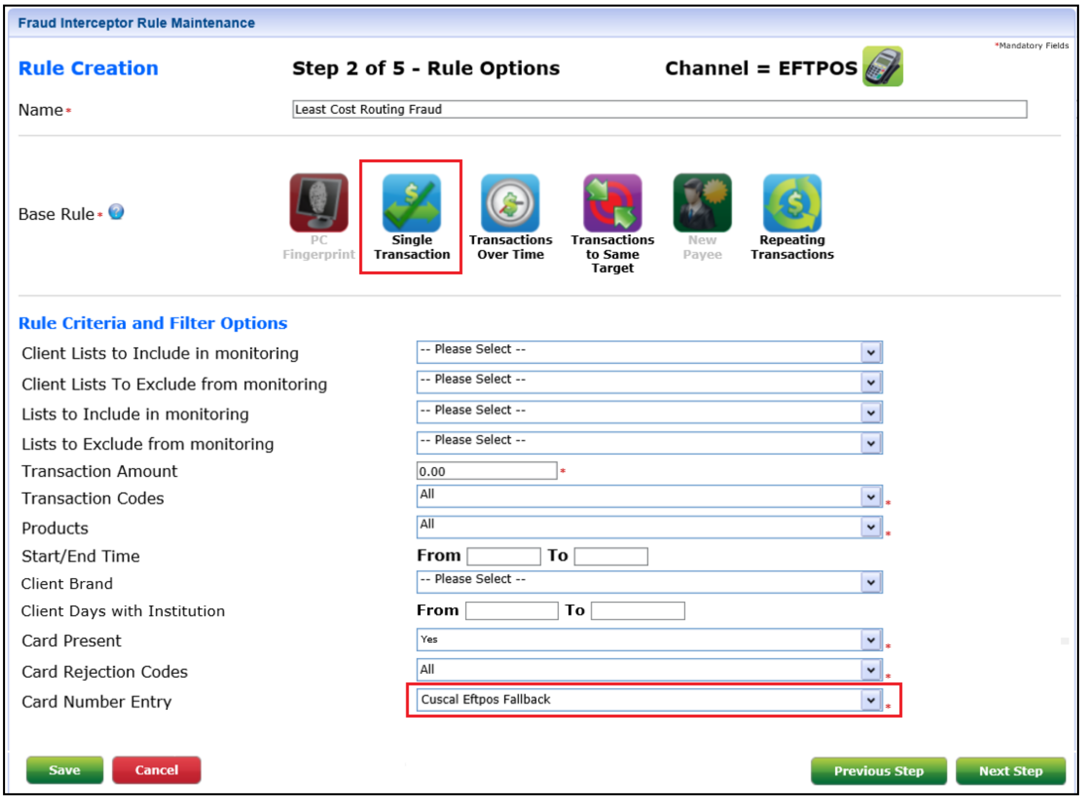
Step 1f Click the **Next Step** button, located at the bottom right of the page, to go to **Step 2 of 5 - Rule Options**.

Rule Options

Step 2a For the **Base Rule**, click on the **Single Transaction** icon.

Step 2b Complete the fields for at least the mandatory items, including setting **Card Present** to 'Yes' and **Card Rejection Codes** to 'All'.

Step 2c You must select 'Cuscal Eftpos Fallback' from the drop-down list of items for the **Card Number Entry** field.



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = EFTPOS**

Name* Least Cost Routing Fraud

Base Rule*

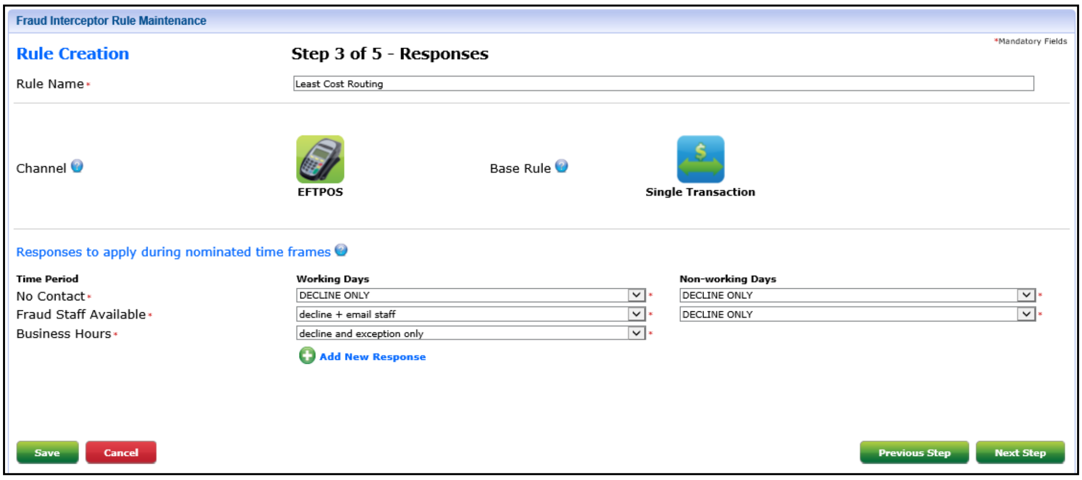
Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount	0.00 *
Transaction Codes	All *
Products	All *
Start/End Time	**From** **To**
Client Brand	-- Please Select --
Client Days with Institution	**From** **To**
Card Present	Yes *
Card Rejection Codes	All *
Card Number Entry	Cuscal Eftpos Fallback *

Step 2d Click the **Next Step** button, located at the bottom right of the page, to go to **Step 3 of 5 - Responses**.

Responses

Step 3a Select the following Responses from the drop-down lists of options for each of the five fields:



Fraud Interceptor Rule Maintenance

Rule Creation **Step 3 of 5 - Responses** *Mandatory Fields

Rule Name* Least Cost Routing

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact*	DECLINE ONLY	DECLINE ONLY
Fraud Staff Available*	decline + email staff	DECLINE ONLY
Business Hours*	decline and exception only	

Notes re some of the Response options:

Decline Only – transaction is declined and not processed to the client's account

- Client knows nothing about what has happened and there is no cost to the business.

Decline and log – allows you to do reporting on any transactions declined as they will be logged as well.

Decline and notify customer – consider whether you need to let the customer know or not. You may choose to replace their card as compromised as a further option, but that can become expensive.

Step 3b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 4 of 5 - Rule Activation**.

Rule Activation

Step 4a Proceed as per normal setting up of a new Rule - i.e., choose when this new Rule is to be activated:

- Do Not Schedule
- Now
- Later Today
- After Today

Step 4b Click the **Next Step** button, located at the bottom right of the page, to go to **Step 5 of 5 - Confirmation**

Confirmation

Step 5a Check all the details of the new Rule displayed on the Confirmation page.

Step 5b Click the green **Finish** button located at the bottom right of the page.

An error message will be displayed if anything has been missed or needs to be corrected.

If required, click the **Previous Step** button go back to earlier steps.

My Viewpoint Channel Rules

The following examples cover a number of scenarios that may be useful for monitoring My Viewpoint transactions.

- My Viewpoint PC Fingerprint and new payee, client without OTP
- More than $5000 in 24 hours to selected BPAY billers
- Sum of My Viewpoint transactions exceeds $10,000 in a 24 hour period
- More than 50 transactions to same external account in three hours
- PC Fingerprint Rule - hold transactions over $5000

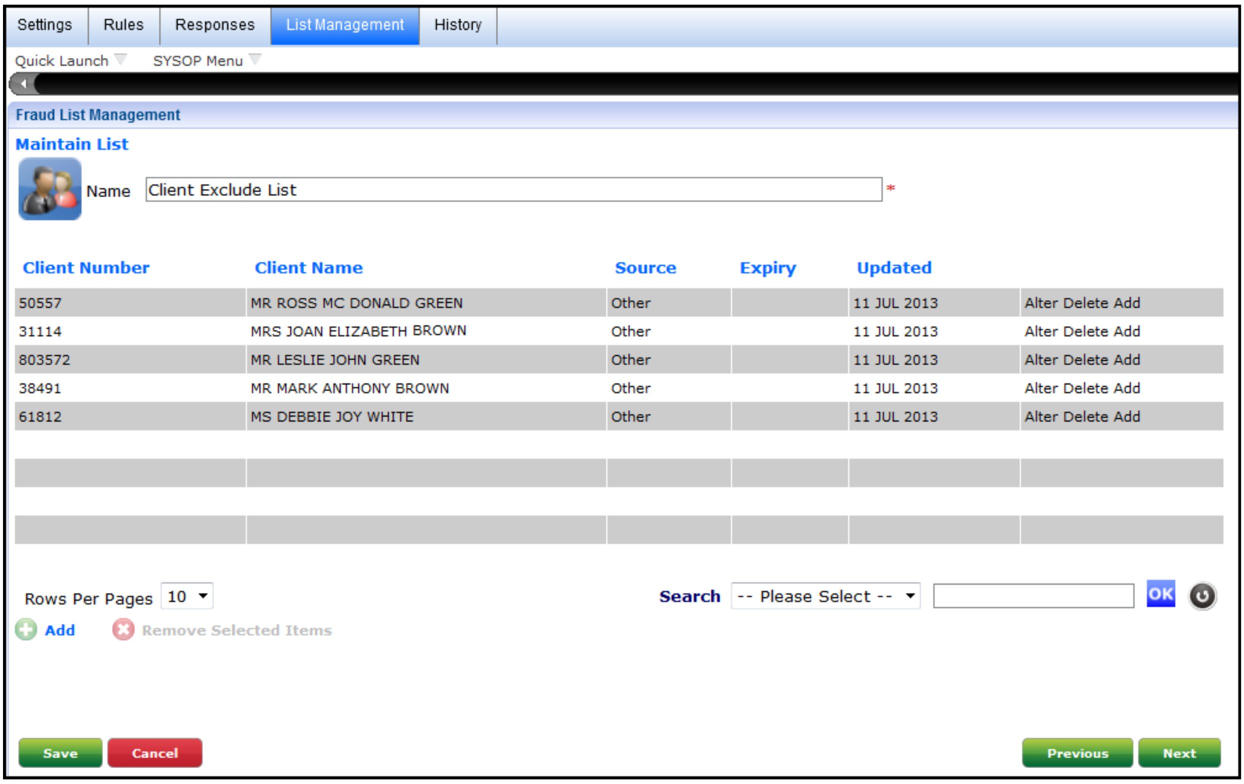
My Viewpoint PC Fingerprint and new payee, client without OTP

This rule is designed to be triggered when two situations occur at the same time, i.e. there are two base rules in operation. These situations are:

- A PC Fingerprint anomaly is encountered, and
- A new payee is added by a client without One Time Password (OTP) security.

If you have clients without OTP who regularly trigger the PC Fingerprint rule and are known to be 'safe', you can optionally exclude these clients with an exclusion list. For example, you may have clients who use multiple PCs, are known to be low risk and who do not have OTP.

Fraud List Management



Fraud List Management

Maintain List

Name: Client Exclude List *

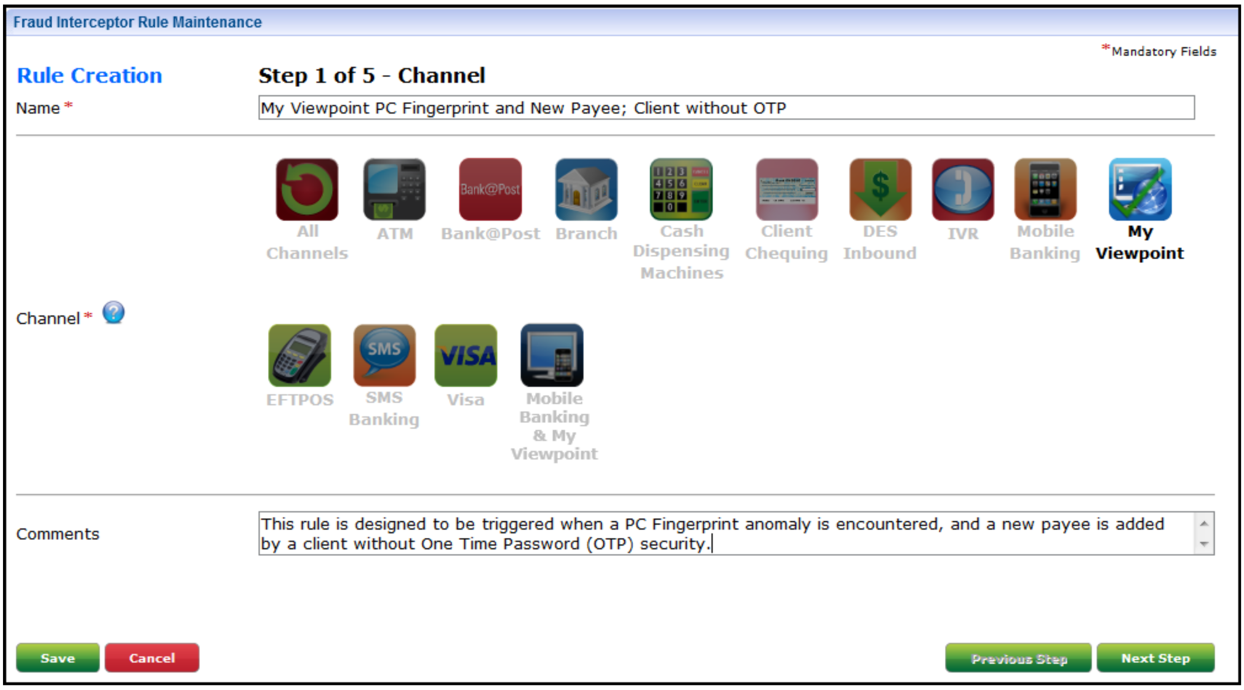
Client Number	Client Name	Source	Expiry	Updated	
50557	MR ROSS MC DONALD GREEN	Other		11 JUL 2013	Alter Delete Add
31114	MRS JOAN ELIZABETH BROWN	Other		11 JUL 2013	Alter Delete Add
803572	MR LESLIE JOHN GREEN	Other		11 JUL 2013	Alter Delete Add
38491	MR MARK ANTHONY BROWN	Other		11 JUL 2013	Alter Delete Add
61812	MS DEBBIE JOY WHITE	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages: 10

Search: -- Please Select --

The Client Exclude List contains the details of clients who will not be included in this rule. You can use this List to cater for known low-risk clients who do not use One Time Passwords (OTP). Clients who are temporarily unable to use OTP (e.g. lost Security Token and waiting for a replacement) may be excluded on a temporary basis by adding an Expiry date.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

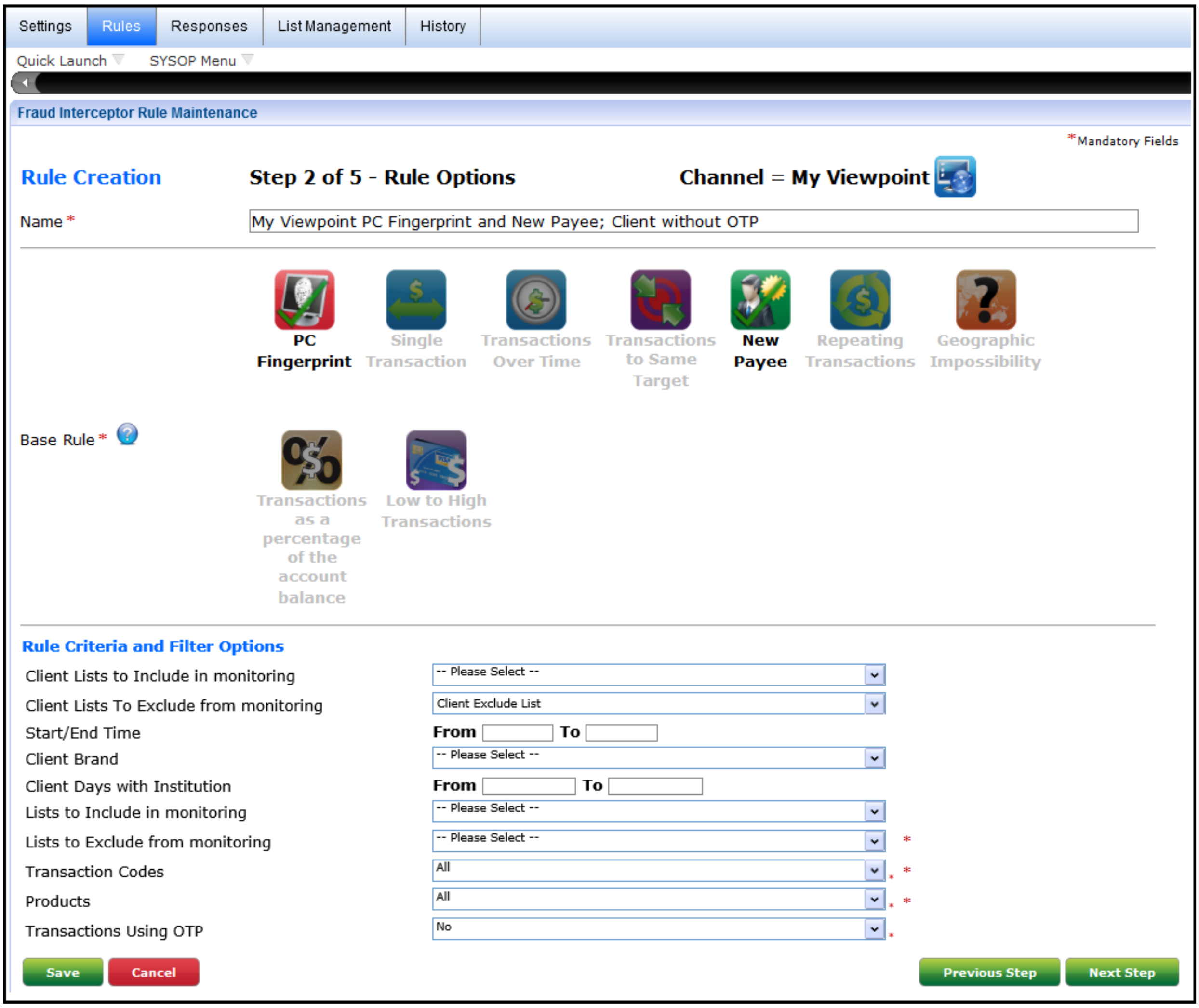
Name * My Viewpoint PC Fingerprint and New Payee; Client without OTP

Channel * My Viewpoint

Comments This rule is designed to be triggered when a PC Fingerprint anomaly is encountered, and a new payee is added by a client without One Time Password (OTP) security.

This rule uses the My Viewpoint channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 2 of 5 - Rule Options

Channel = My Viewpoint

Name * My Viewpoint PC Fingerprint and New Payee; Client without OTP

Base Rule * PC Fingerprint, New Payee

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Client Exclude List
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select -- *
Transaction Codes	All *
Products	All *
Transactions Using OTP	No

This rule uses two Base Rules, 'PC Fingerprint' and 'New Payee'.

The following criteria and filter options have been specified:

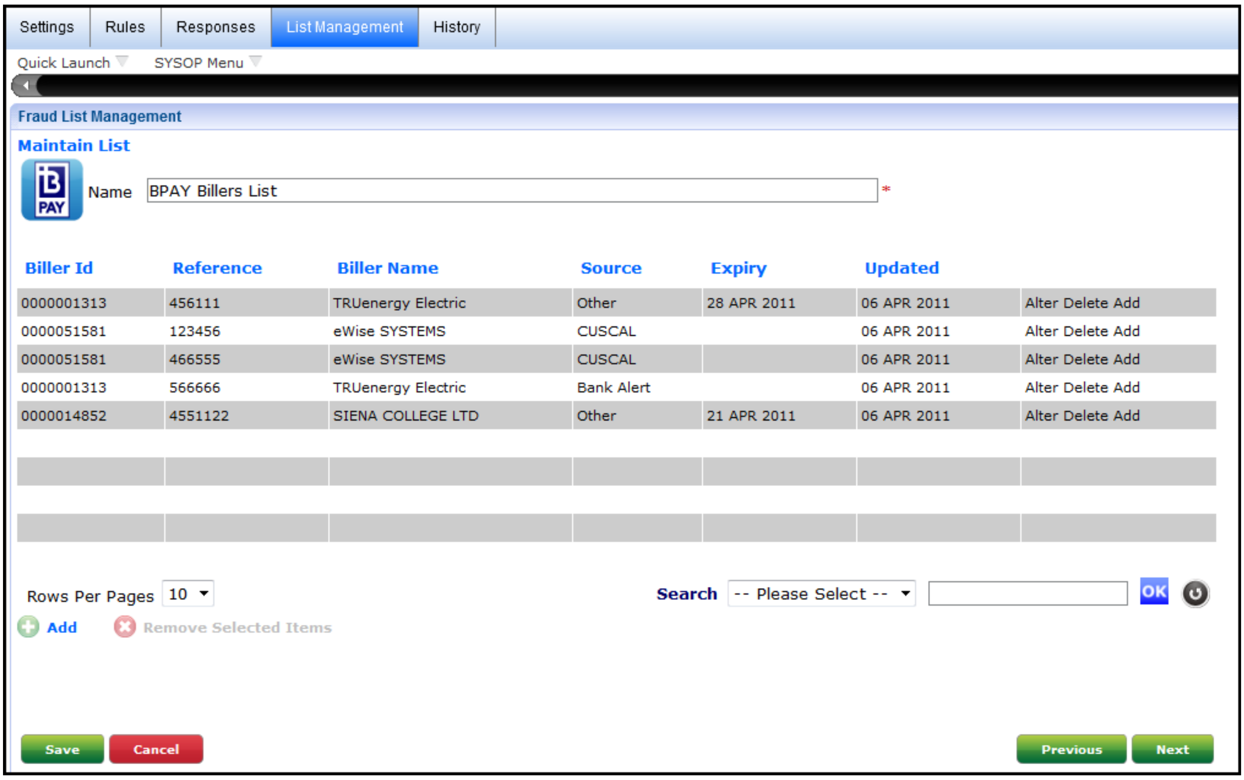
Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring**	A client list (Include or Exclude) is optional and if both are left unselected, all clients will be included in this rule. In this example, the 'Client Exclude List' has been used to exclude known 'safe' clients without One Time Passwords. When an exclusion list is used, the inclusion list filed should be left as "-- Please Select --".
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Lists to Include in monitoring **Lists to Exclude from Monitoring**	Additional (i.e. not client), optional lists may be used to include or exclude this rule from monitoring. If both are left unselected, all matches will be included in this rule.
Transaction Codes	'All' transactions are included in this rule; however, you may prefer to select only credit transactions.
Products	'All' has been selected; however, if you only have one or two product types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Transactions Using OTP	'No' has been selected to capture transactions from clients who are not using One Time Passwords (OTP).

More than $5000 in 24 hours to selected BPAY billers

This rule is designed to be triggered when a set total amount of transactions is reached in a specified time to BPAY billers on a list. Before setting up this rule, you need to create (or have an existing) list of BPAY Billers using the List Management option.

In this example, the rule is only being targeted to My Viewpoint users; however; you could also create this rule for All Channels in order to capture transactions from My Viewpoint, Mobile Banking (including Ultracs App 2 and Ultracsapp), IVR and Ultracs within a single rule. You could also create this rule for the Mobile Banking & My Viewpoint channel in order to capture transactions only from Mobile Banking (including Ultracs App 2 and Ultracsapp) and My Viewpoint.

Fraud List Management



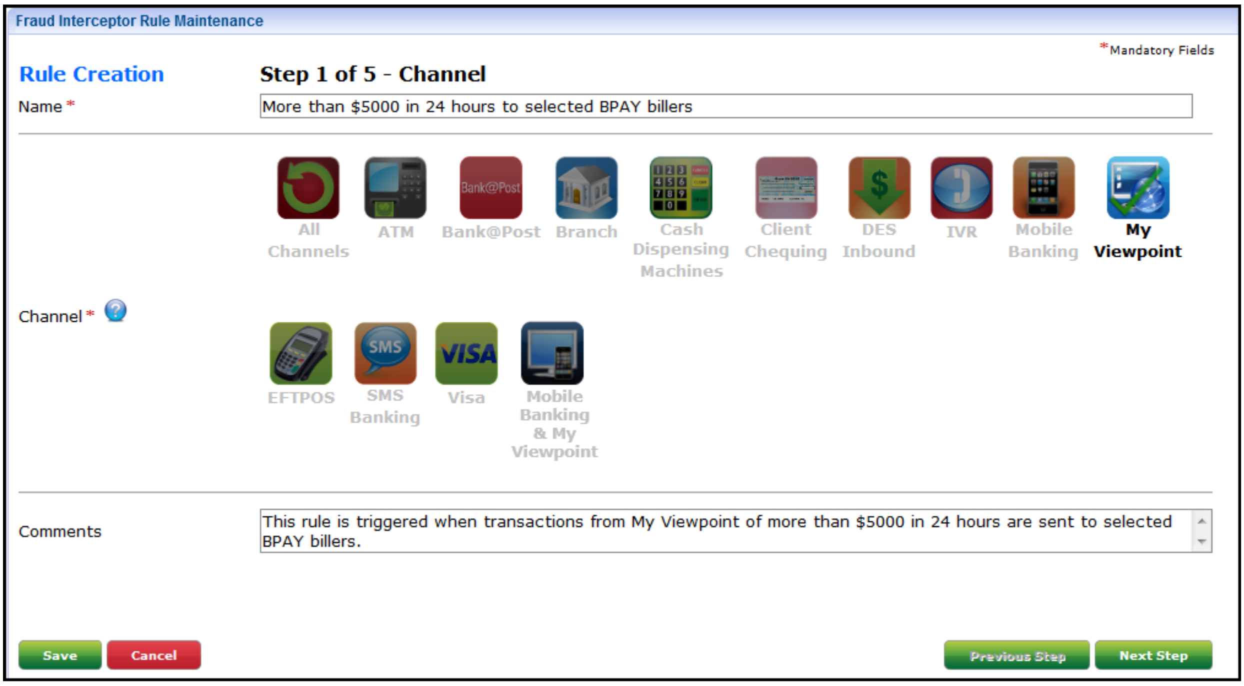
Name BPAY Billers List *

Biller Id	Reference	Biller Name	Source	Expiry	Updated	
0000001313	456111	TRUenergy Electric	Other	28 APR 2011	06 APR 2011	Alter Delete Add
0000051581	123456	eWise SYSTEMS	CUSCAL		06 APR 2011	Alter Delete Add
0000051581	466555	eWise SYSTEMS	CUSCAL		06 APR 2011	Alter Delete Add
0000001313	566666	TRUenergy Electric	Bank Alert		06 APR 2011	Alter Delete Add
0000014852	4551122	SIENA COLLEGE LTD	Other	21 APR 2011	06 APR 2011	Alter Delete Add

Rows Per Pages 10

A BPAY list called 'BPAY Billers List' is used in this example.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

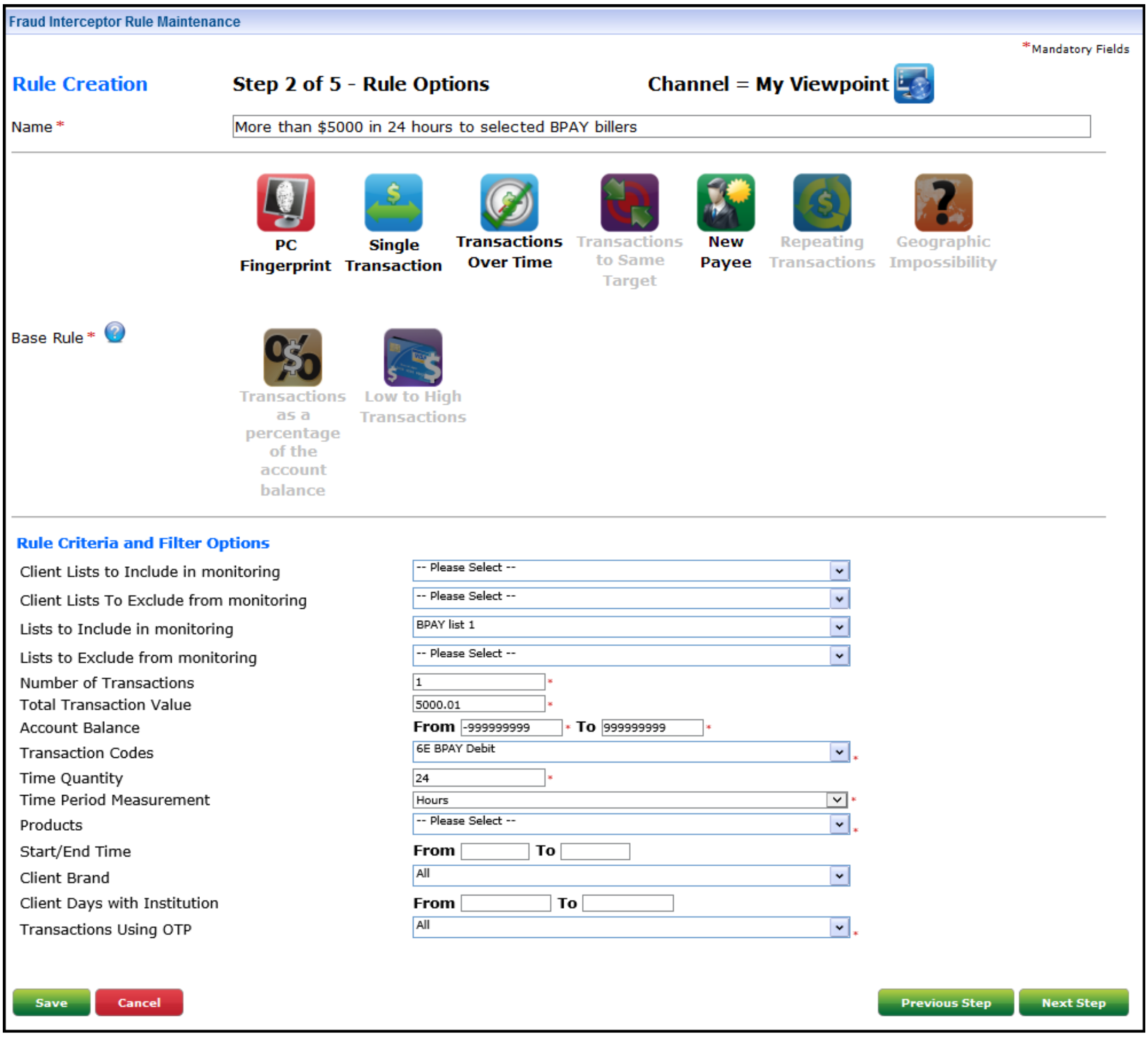
Name * More than $5000 in 24 hours to selected BPAY billers

Channel *

Comments: This rule is triggered when transactions from My Viewpoint of more than $5000 in 24 hours are sent to selected BPAY billers.

This rule uses the My Viewpoint channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = My Viewpoint**

Name *: More than $5000 in 24 hours to selected BPAY billers

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	BPAY list 1
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	1 *
Total Transaction Value	5000.01 *
Account Balance	From -999999999 * To 999999999 *
Transaction Codes	6E BPAY Debit *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	-- Please Select -- *
Start/End Time	From To
Client Brand	All
Client Days with Institution	From To
Transactions Using OTP	All *

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in monitoring **Client Lists to Exclude from monitoring** **Lists to Include in monitoring** **Lists to Exclude from monitoring**	The "BPAY Billers List" is selected from the 'Lists to Include in monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --" unless you wanted to add or exclude clients from monitoring.
Number of Transactions	If you enter '1' into this field, any number of transactions will be considered.
Total Transaction Value	As this rule is to apply to the sum of transactions more than $5,000 and the field itself will include the value entered, you need to enter 5000.01 (or 5001 if you are not concerned with cents).

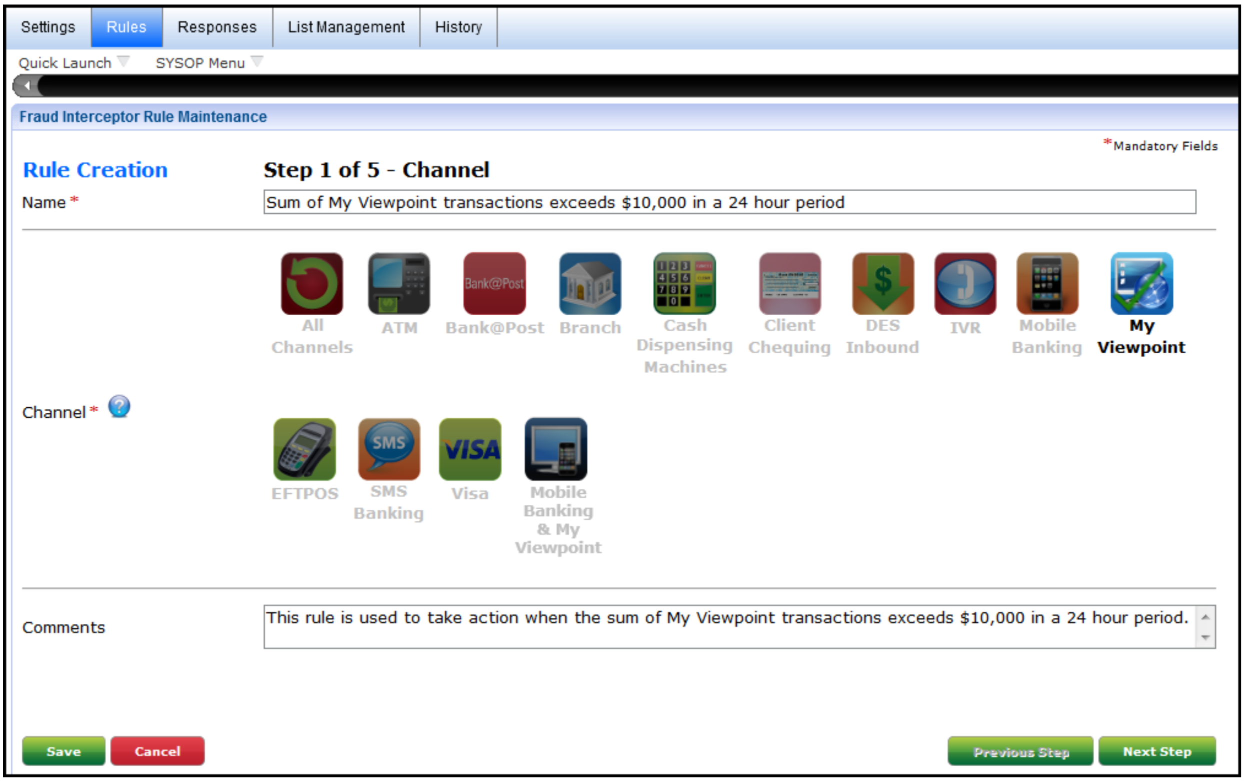
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. In this instance, the BPAY debit transaction code is selected.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected; however, you could just as well have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two product types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Transactions Using OTP	'All' has been selected to capture transactions from both clients using One Time Passwords (OTP) and those not using OTP. If you considered OTP users should be excluded due to the lower risk, you could have selected 'No' from the drop-down list.

Sum of My Viewpoint transactions exceeds $10,000 in a 24 hour period

This rule is designed to be triggered when the total of transactions from My Viewpoint exceeds a set amount in any 24 hour period.

If required, you could optionally exclude clients who regularly perform large value transactions and are expected to present a low risk.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



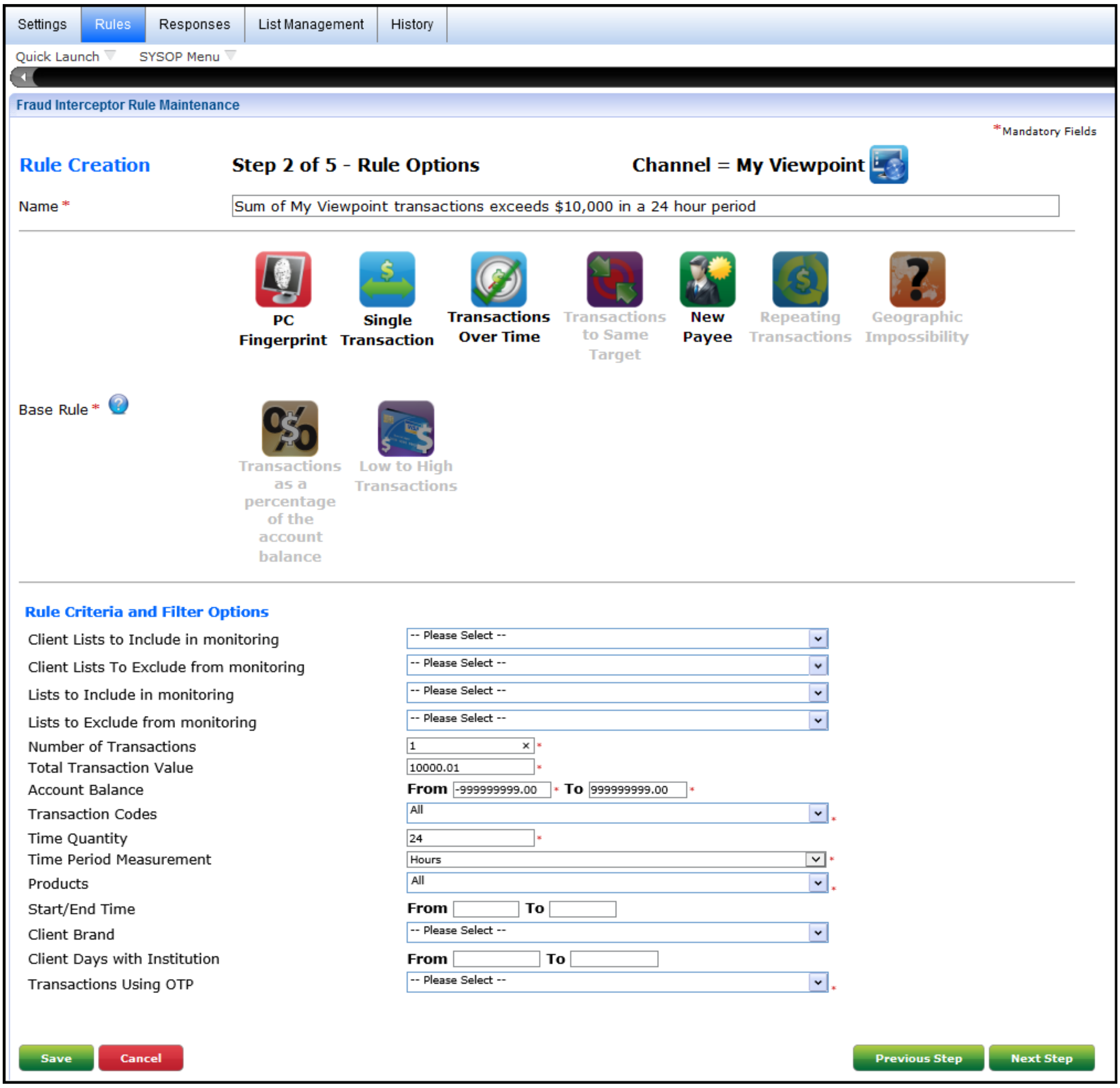
Name * Sum of My Viewpoint transactions exceeds $10,000 in a 24 hour period

Channel * My Viewpoint

Comments This rule is used to take action when the sum of My Viewpoint transactions exceeds $10,000 in a 24 hour period.

This rule uses the My Viewpoint channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = My Viewpoint**

Name *: Sum of My Viewpoint transactions exceeds $10,000 in a 24 hour period

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	1 *
Total Transaction Value	10000.01 *
Account Balance	From -999999999.00 * To 999999999.00 *
Transaction Codes	All *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Transactions Using OTP	-- Please Select -- *

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	There are no lists selected in this example; however, you could use client and other lists to suit your needs, for example, you could use a client list to exclude clients you know are low risk and frequently have a transaction pattern that would falsely trigger this rule.
Number of Transactions	If you enter '1' into this field, any number of transactions will be considered.

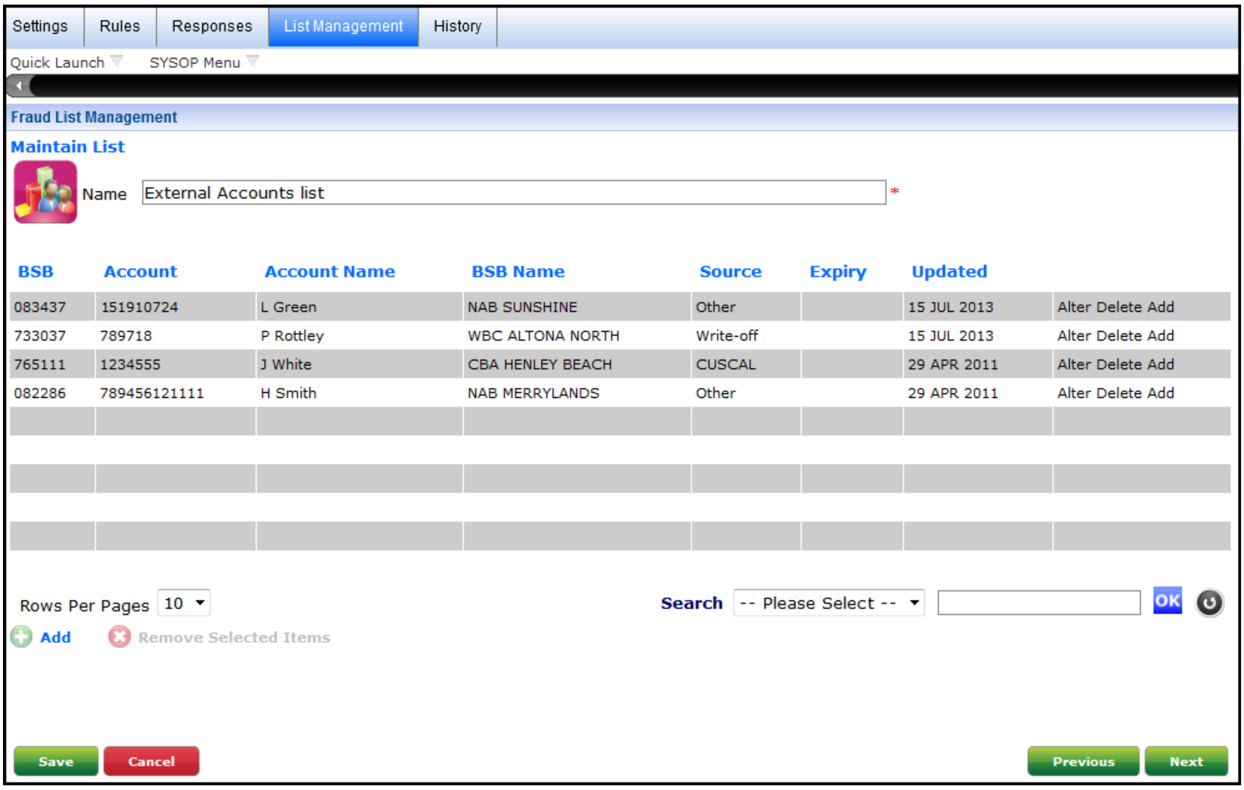
Total Transaction Value	As this rule is to apply to the sum of transactions over $10,000 and the field itself will include the value entered, you need to enter 10000.01 (or 10001 if you are not concerned with cents).
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. The minimum you are likely to require are VISA Cash Advance and VISA Retail Purchase codes. You may also include other codes such as ATM/POS Withdrawal if you consider those codes appropriate.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected; however, you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two product types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	These fields would normally be left blank in this rule.
Client Brand	If Client Branding is applicable, select one or more brand(s) from the drop-down list. The Rule will only apply to the selected brand(s). 'All' is the default.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Transactions Using OTP	'All' has been selected to capture transactions from both clients using One Time Passwords (OTP) and those not using OTP. If you considered OTP users should be excluded due to the lower risk, you could have selected 'No' from the drop-down list.

More than 50 transactions to same external account in three hours

This rule is triggered when there are more than 50 transactions to the same target external account (from any client), excluding specific known safe accounts, in a 3- hour period.

You will need to create an Accounts List to known safe accounts in order to exclude these accounts from monitoring.

Fraud List Management



Name External Accounts list *

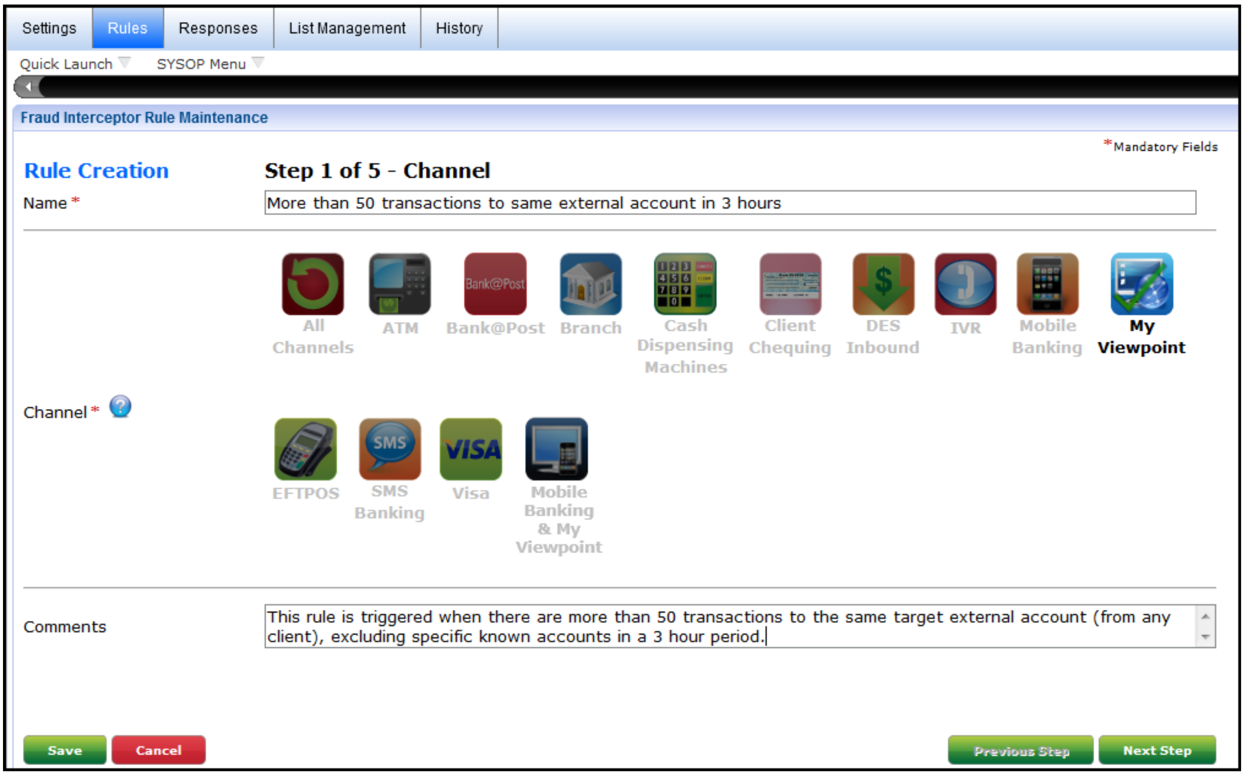
BSB	Account	Account Name	BSB Name	Source	Expiry	Updated	
083437	151910724	L Green	NAB SUNSHINE	Other		15 JUL 2013	Alter Delete Add
733037	789718	P Rottley	WBC ALTONA NORTH	Write-off		15 JUL 2013	Alter Delete Add
765111	1234555	J White	CBA HENLEY BEACH	CUSCAL		29 APR 2011	Alter Delete Add
082286	789456121111	H Smith	NAB MERRYLANDS	Other		29 APR 2011	Alter Delete Add

Rows Per Pages 10

Search -- Please Select --

This External Accounts List contains the bank details for accounts that are known to be safe. Transactions to these accounts will be excluded from the rule.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



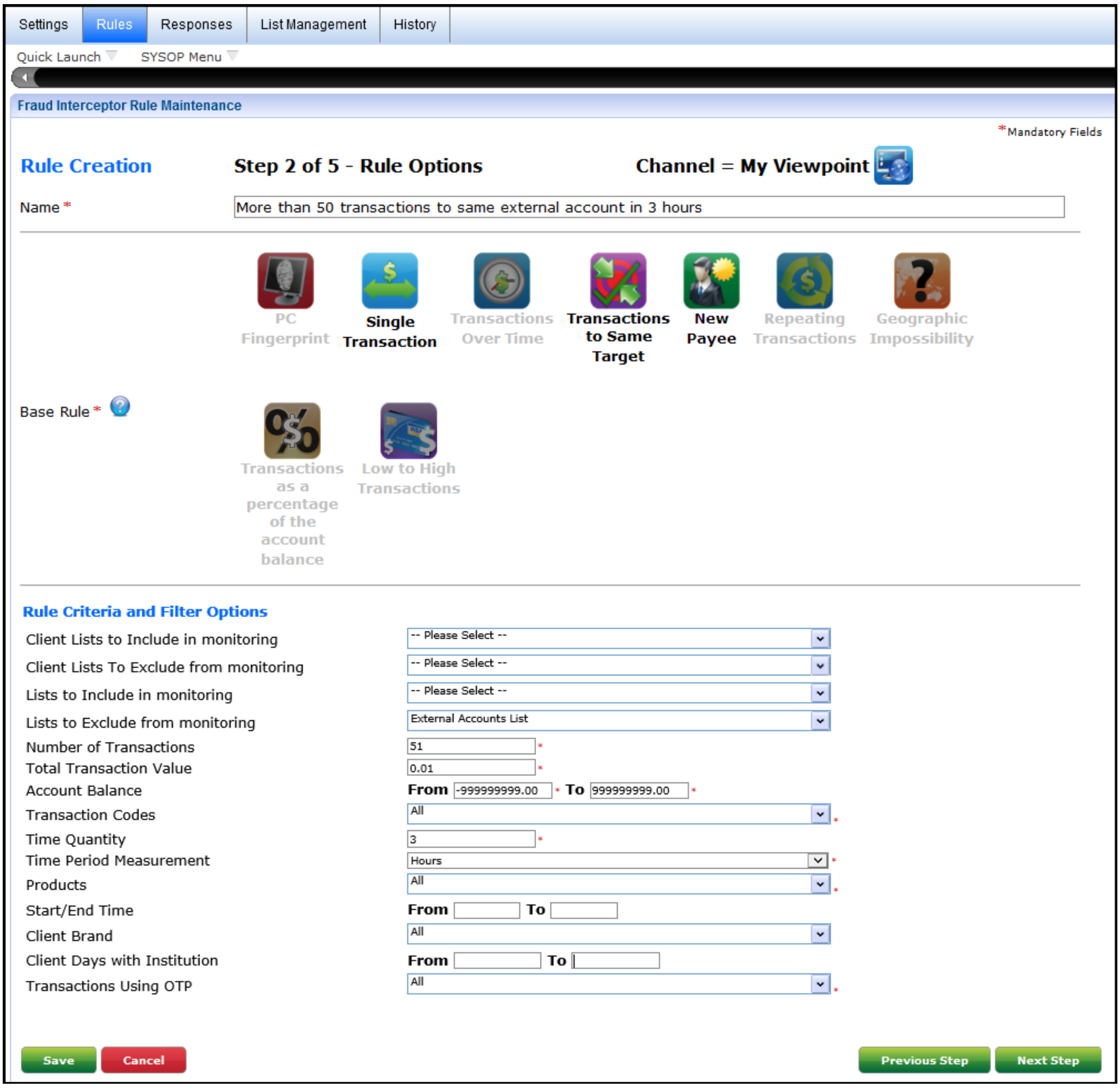
Name *: More than 50 transactions to same external account in 3 hours

Channel *: My Viewpoint

Comments: This rule is triggered when there are more than 50 transactions to the same target external account (from any client), excluding specific known accounts in a 3 hour period.

This rule uses the My Viewpoint channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



*Mandatory Fields

Rule Creation

Step 2 of 5 - Rule Options

Channel = My Viewpoint

Name *	More than 50 transactions to same external account in 3 hours
Base Rule *	Transactions to Same Target

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	External Accounts List
Number of Transactions	51 *
Total Transaction Value	0.01 *
Account Balance	From -999999999.00 * To 999999999.00 *
Transaction Codes	All *
Time Quantity	3 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	All
Client Days with Institution	From To
Transactions Using OTP	All *

This rule uses the Base Rule 'Transactions to Same Target'.

The following criteria and filter options have been specified:

Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	Select the Accounts List you created for this rule from the 'Lists to Exclude from monitoring' drop-down list. 'Lists to Include in monitoring' should be left as "-- Please Select --". A client list (Include or Exclude) is optional and if both are left unselected, all clients will be included in this rule.
Number of Transactions	The scenario is to be triggered when there are more than 50 transactions; therefore, '51' is entered into this field.

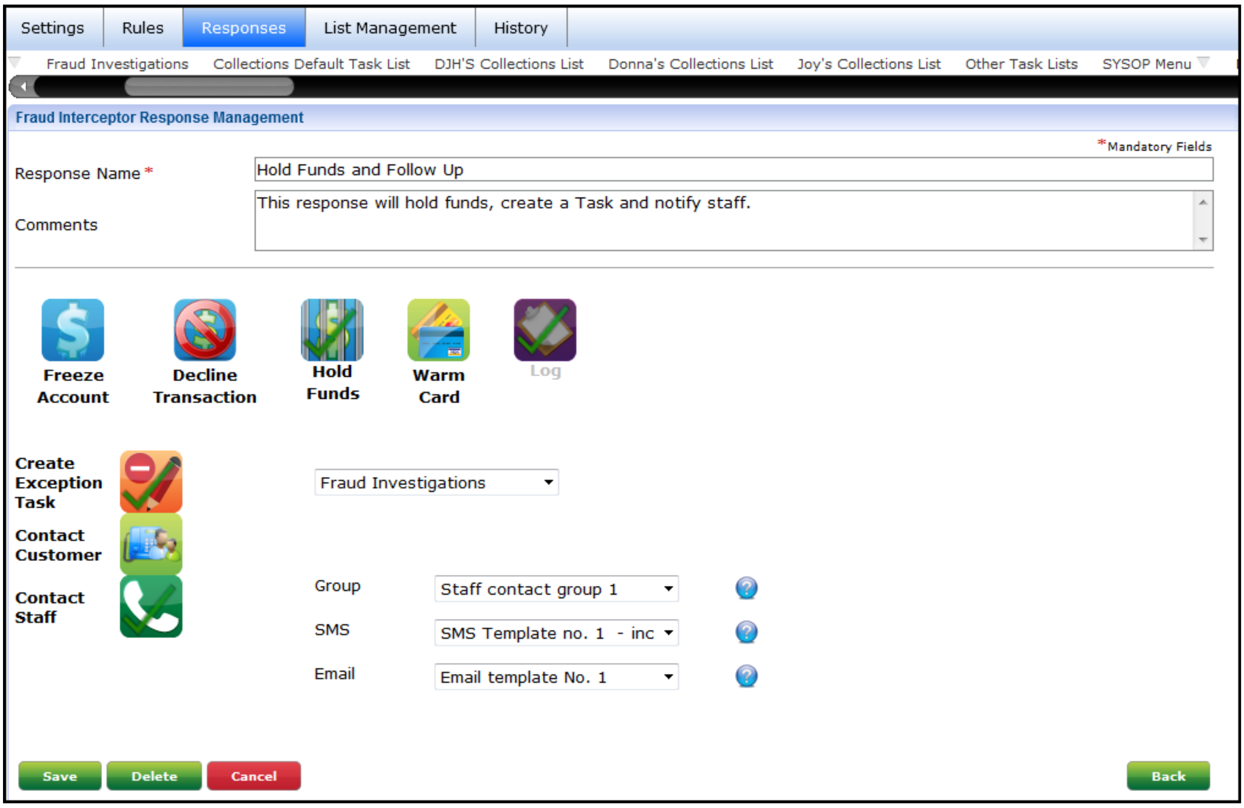
Total Transaction Value	Any value of the transactions should be allowed to trigger this scenario; however, it is unlikely they will have a negative overall total so you may as well enter 0.01.
Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	'All' transactions are included in this rule; however, you may prefer to select only credit transactions.
Time Quantity **Time Period Measurement**	These two fields are used together. In this example, '3' and 'Hours' have been selected.
Products	'All' has been selected; however, if you only have one or two products types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	These fields would normally be left blank in this rule.
Client Brand	If Client Branding is applicable, select one or more brand(s) from the drop-down list. The Rule will only apply to the selected brand(s). 'All' is the default.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.
Transactions Using OTP	'All' has been selected to capture transactions from both clients using One Time Passwords (OTP) and those not using OTP. If you considered OTP users should be excluded due to the lower risk, you could have selected 'No' from the drop-down list.

PC Fingerprint Rule - hold transactions over $5000

This rule is triggered when a PC Fingerprint anomaly is encountered when trying to perform a transaction with a value of more than $5000. The funds will be held and an exception will be raised so the appropriate action may be taken.

Response - Hold Funds and Follow Up

The following shows the 'Hold Funds and Follow Up' response which was created to hold the funds, create an exception task and contact staff.



Fraud Interceptor Response Management

*Mandatory Fields

Response Name * Hold Funds and Follow Up

Comments This response will hold funds, create a Task and notify staff.

Create Exception Task: Fraud Investigations

Contact Customer

Contact Staff

Group: Staff contact group 1

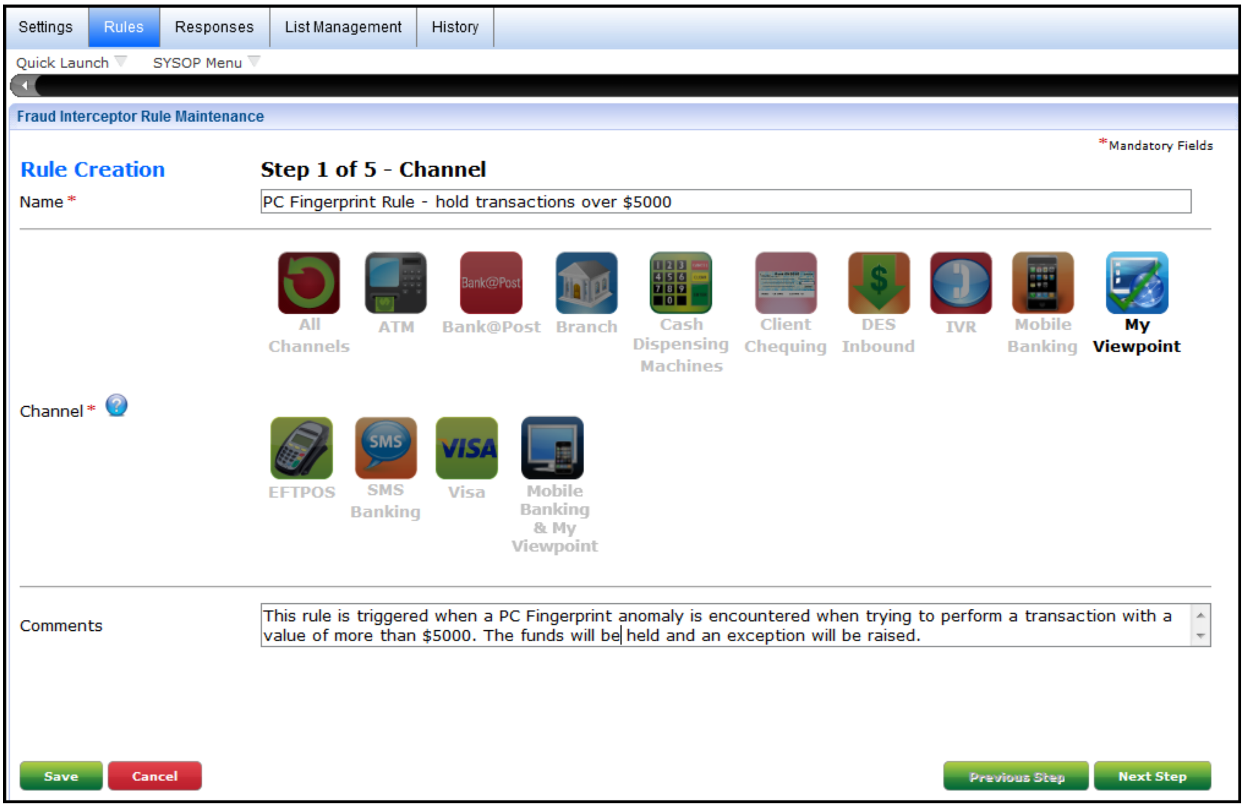
SMS: SMS Template no. 1 - inc

Email: Email template No. 1

It is best to create the response before creating the rule.

Note the response will add an Exception Task to the Fraud Investigations Task List and also contact staff who are part of the 'Staff contact group 1'. Contact is made by way of SMS and Email messages. Templates are used to determine the content of the messages. Additional information on setting up Groups and SMS and Email templates can be found in the **Fraud Interceptor User Manual**.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



*Mandatory Fields

Rule Creation

Step 1 of 5 - Channel

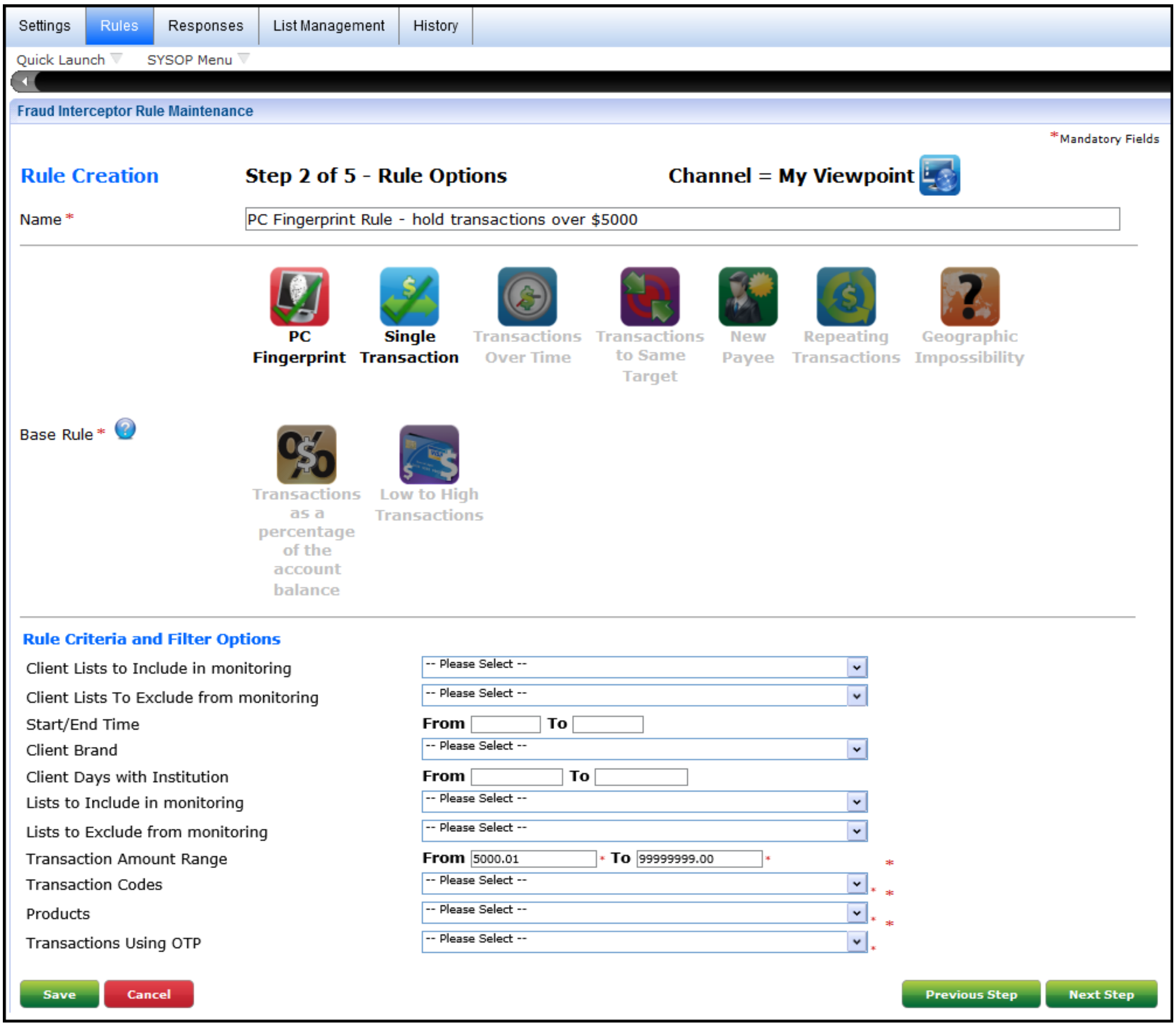
Name * PC Fingerprint Rule - hold transactions over $5000

Channel *

Comments This rule is triggered when a PC Fingerprint anomaly is encountered when trying to perform a transaction with a value of more than $5000. The funds will be held and an exception will be raised.

This rule uses the My Viewpoint channel.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Fraud Interceptor Rule Maintenance

*Mandatory Fields

Rule Creation **Step 2 of 5 - Rule Options** **Channel = My Viewpoint**

Name * PC Fingerprint Rule - hold transactions over $5000

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	-- Please Select --
Start/End Time	From To
Client Brand	-- Please Select --
Client Days with Institution	From To
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Transaction Amount Range	From 5000.01 * To 99999999.00 *
Transaction Codes	-- Please Select -- *
Products	-- Please Select -- *
Transactions Using OTP	-- Please Select -- *

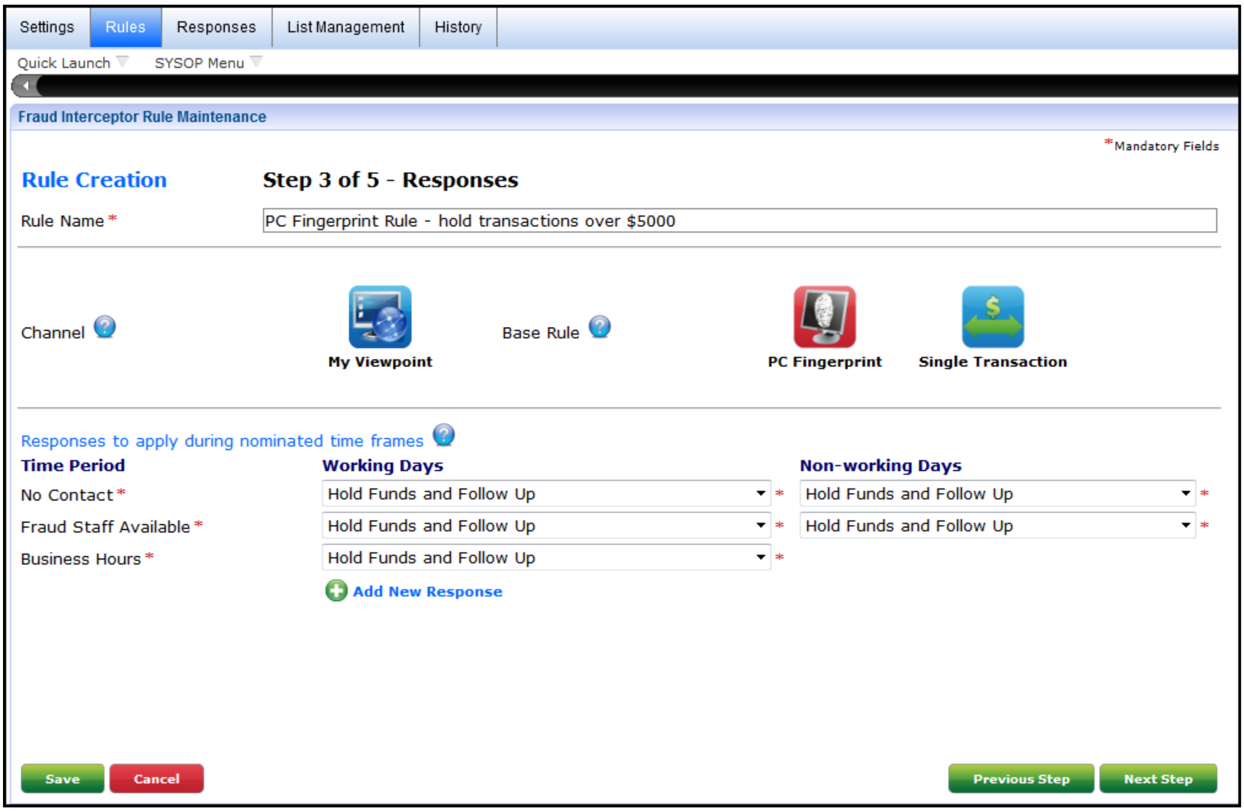
This rule uses two Base Rules, 'PC Fingerprint' and 'Single Transaction'.

The following criteria and filter options have been specified:

Client Lists to Include in monitoring **Client Lists to Exclude from monitoring**	A client list (Include or Exclude) is optional and if both are left unselected, all clients will be included in this rule.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.

Lists to Include in monitoring **Lists to Exclude from Monitoring**	Additional (i.e. not client), optional lists may be used to include or exclude this rule from monitoring. If both are left unselected, all matches will be included in this rule.
Transaction Amount Range	This rule is to apply for transactions of more than $5000; therefore, '5000.01' is entered into the From field and the maximum value in the To field.
Transaction Codes	'All' transactions are included in this rule; however, you may prefer to select only credit transactions.
Products	'All' has been selected; however, if you only have one or two product types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Transactions Using OTP	'All' has been selected to capture transactions from both clients using One Time Passwords (OTP) and those not using OTP. If you considered OTP users should be excluded due to a lower risk, you could have selected 'No' from the drop-down list.

Fraud Interceptor Rule Maintenance - Step 3 of 5 - Responses



Rule Creation

Step 3 of 5 - Responses

Rule Name * PC Fingerprint Rule - hold transactions over $5000

Channel: My Viewpoint

Base Rule: PC Fingerprint, Single Transaction

Responses to apply during nominated time frames

Time Period	Working Days	Non-working Days
No Contact *	Hold Funds and Follow Up *	Hold Funds and Follow Up *
Fraud Staff Available *	Hold Funds and Follow Up *	Hold Funds and Follow Up *
Business Hours *	Hold Funds and Follow Up *	

Add New Response

The responses are used to automatically apply the actions required. In this case to hold the funds and contact staff by various means and provide a follow-up action. This is done using the 'Hold and Follow Up' response. In this example, the same response has been applied to all time periods and working and non-working days. If required, you could have different responses for different time periods.

As with all responses where a staff action is required, a Task is generated and added to an appropriate Task List which is defined in the response.

All Channels

The following examples are scenarios that may be useful for monitoring all transactions.

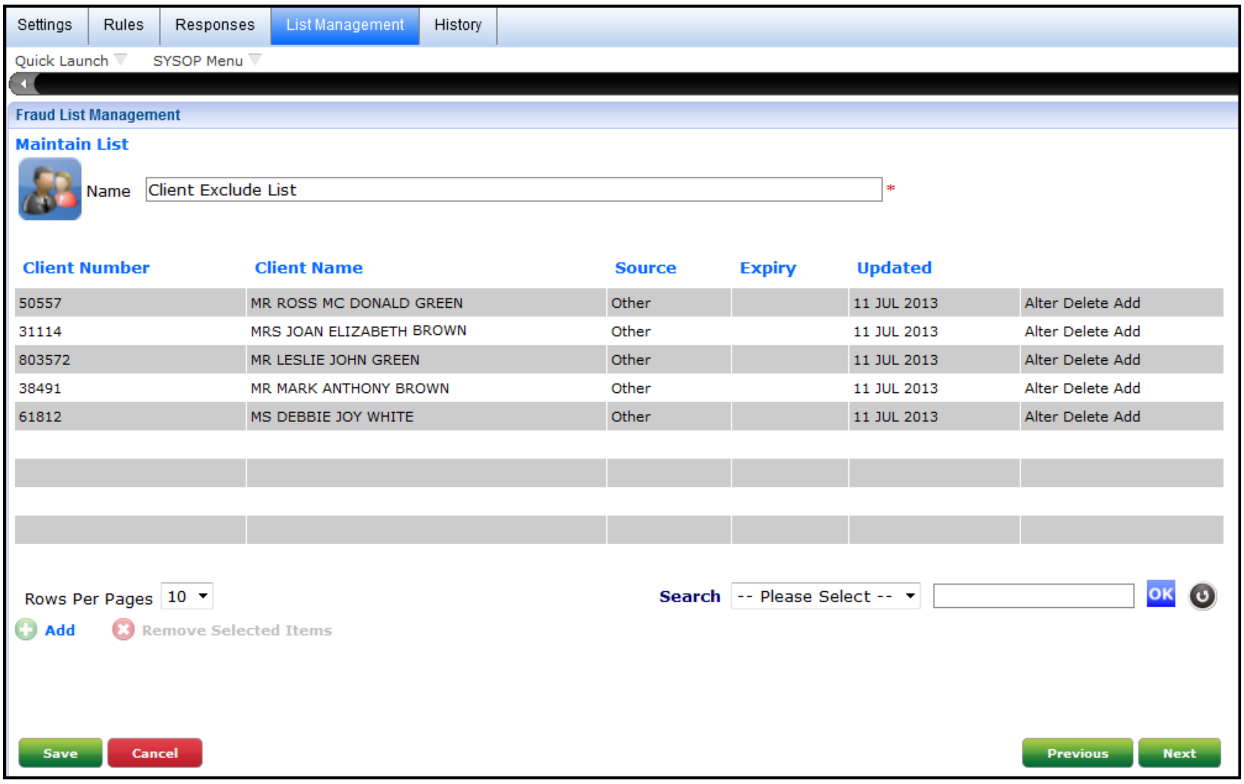
- Total of debit transactions exceeds $25,000 in 24 hours
- All transactions as a percentage of balance

Total of debit transactions exceeds $25,000 in 24 hours

This rule is designed to be triggered when the total of all debit transactions (excluding reversals, fees, taxes and financial institution charges) for a client exceeds a specified value within a set time period.

As you are likely to have a number of clients who may be expected to exceed this value, this rule would probably need to be used in conjunction with a client exclusion list.

Fraud List Management



Name Client Exclude List *

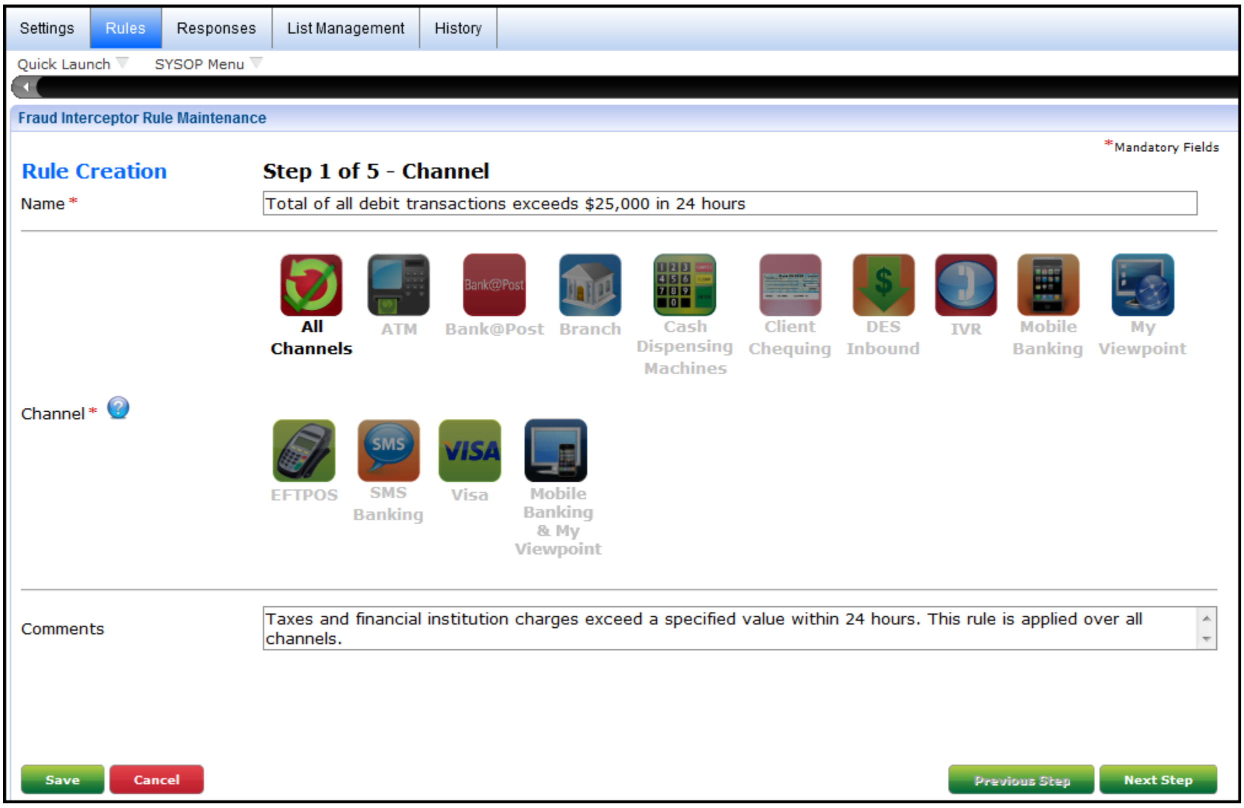
Client Number	Client Name	Source	Expiry	Updated	
50557	MR ROSS MC DONALD GREEN	Other		11 JUL 2013	Alter Delete Add
31114	MRS JOAN ELIZABETH BROWN	Other		11 JUL 2013	Alter Delete Add
803572	MR LESLIE JOHN GREEN	Other		11 JUL 2013	Alter Delete Add
38491	MR MARK ANTHONY BROWN	Other		11 JUL 2013	Alter Delete Add
61812	MS DEBBIE JOY WHITE	Other		11 JUL 2013	Alter Delete Add

Rows Per Pages 10

Search -- Please Select --

The Client Exclude List contains the details of clients who will not be included in this rule. You can use this List to cater for known low-risk clients who you would expect to trigger this rule on recurring basis.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel



Rule Creation

Step 1 of 5 - Channel

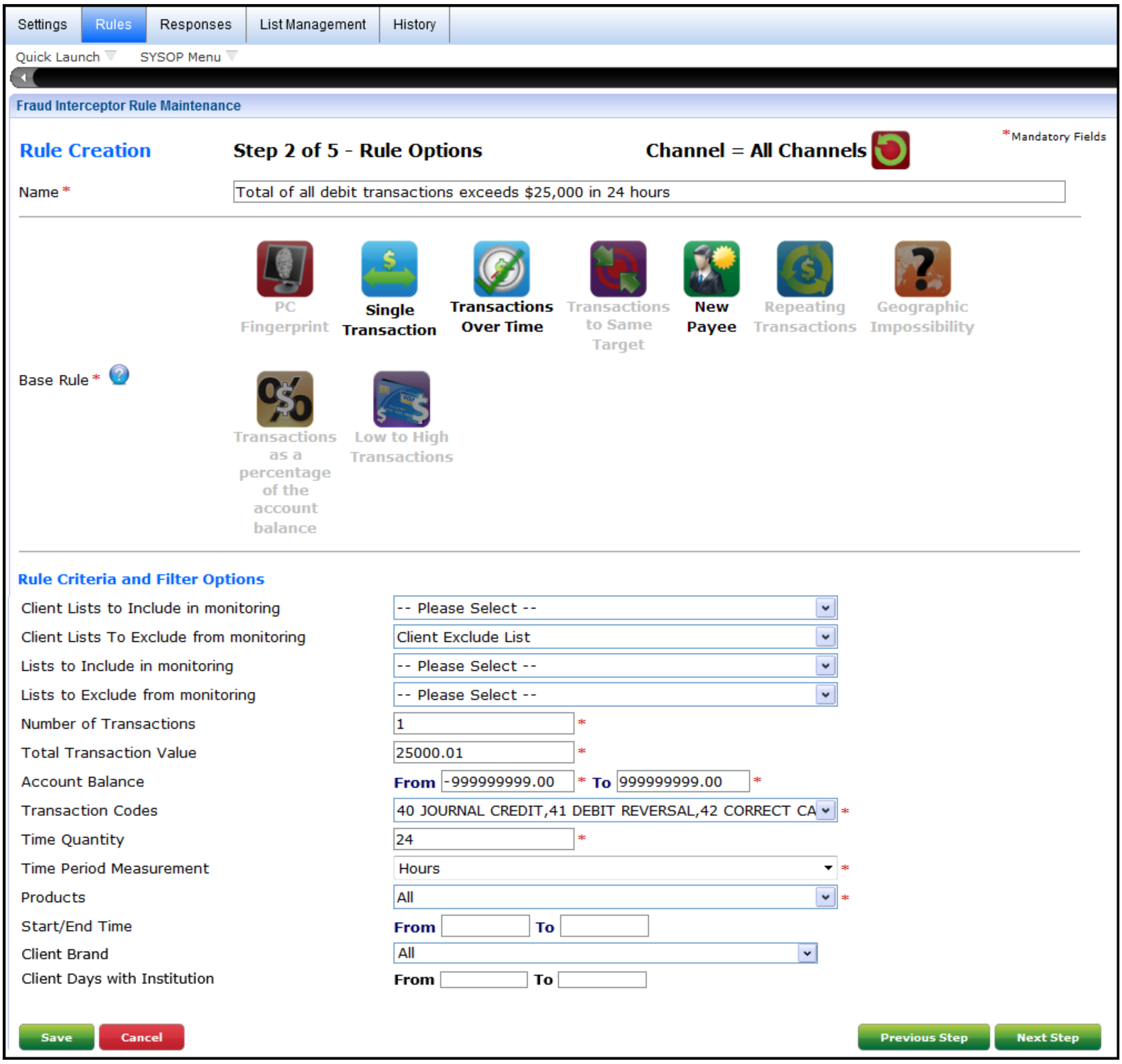
Name * Total of all debit transactions exceeds $25,000 in 24 hours

Channel * All Channels

Comments Taxes and financial institution charges exceed a specified value within 24 hours. This rule is applied over all channels.

This rule uses All Channels.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Rule Creation Step 2 of 5 - Rule Options Channel = All Channels *Mandatory Fields

Name * Total of all debit transactions exceeds $25,000 in 24 hours

Base Rule *

Rule Criteria and Filter Options

Client Lists to Include in monitoring	-- Please Select --
Client Lists To Exclude from monitoring	Client Exclude List
Lists to Include in monitoring	-- Please Select --
Lists to Exclude from monitoring	-- Please Select --
Number of Transactions	1 *
Total Transaction Value	25000.01 *
Account Balance	From -999999999.00 * To 999999999.00 *
Transaction Codes	40 JOURNAL CREDIT,41 DEBIT REVERSAL,42 CORRECT CA *
Time Quantity	24 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	All
Client Days with Institution	From To

This rule uses the Base Rule 'Transactions Over Time'.

The following criteria and filter options have been specified:

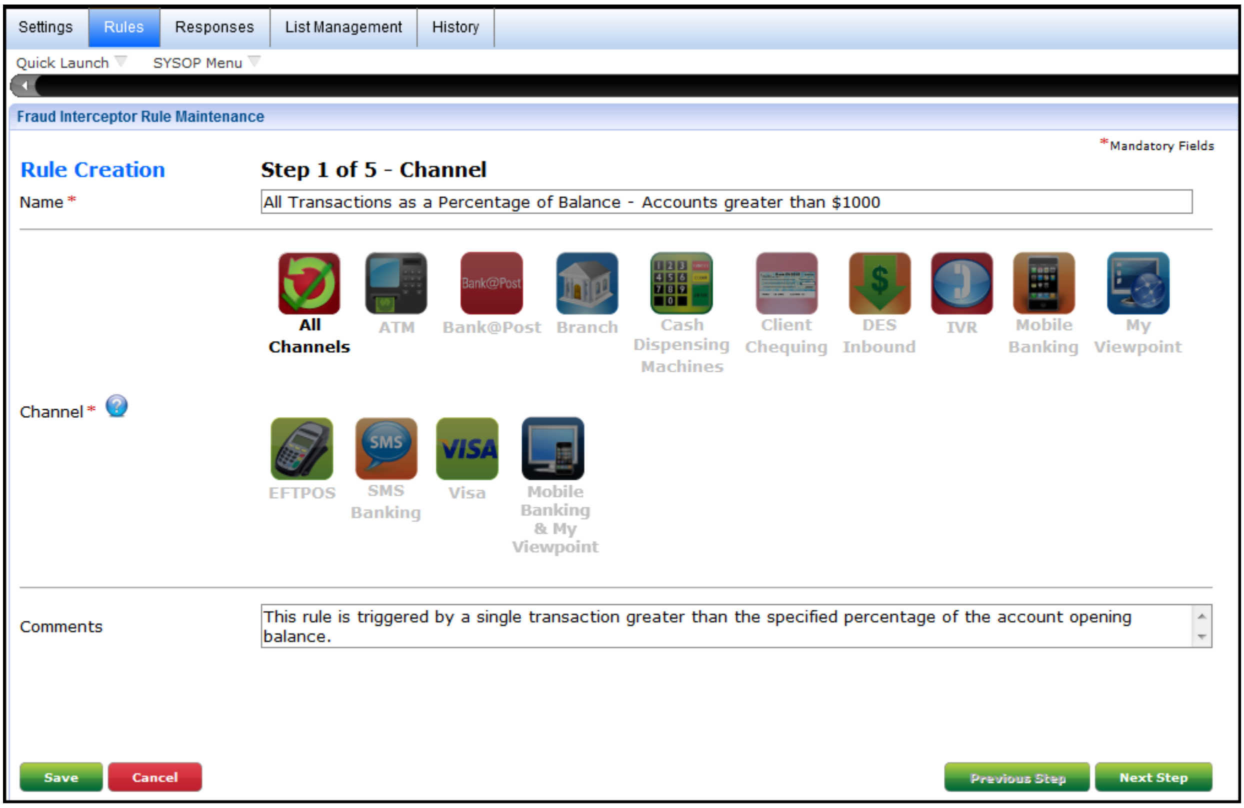
Client Lists to Include in Monitoring **Client Lists to Exclude from Monitoring** **Lists to Include in monitoring** **Lists to Exclude from Monitoring**	You can optionally exclude known 'safe' clients. This has been done by selecting the "Client Exclude List" from the 'Client List to Exclude from Monitoring' drop-down list. The other lists options will normally be left as "-- Please Select --".
Number of Transactions	If you enter '1' into this field, any number of transactions will be considered.
Total Transaction Value	As this rule is to apply to the sum of transactions over $25,000 and the field itself will include the value entered, you need to enter 25000.01 (or 25001 if you are not concerned with cents).

Account Balance	The Account Balance values can be any values you consider appropriate for this rule.
Transaction Codes	Select the appropriate Transaction Codes from the drop-down list. This should include all debit transaction codes except those that are being excluded - such as reversals, fees, taxes and financial institution charges.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '24' and 'Hours' have been selected; however, you could also have used '1' and 'Days'.
Products	'All' has been selected; however, if you only have one or two products types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	These fields would normally be left blank in this rule.
ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.

All transactions as a percentage of balance

This rule will be triggered by a transaction that leaves the account with no more than 10% of the original balance when the original balance is at least $1000. In this example, a 1 hour time period will be considered before the first and last transaction.

Fraud Interceptor Rule Maintenance - Step 1 of 5 - Channel

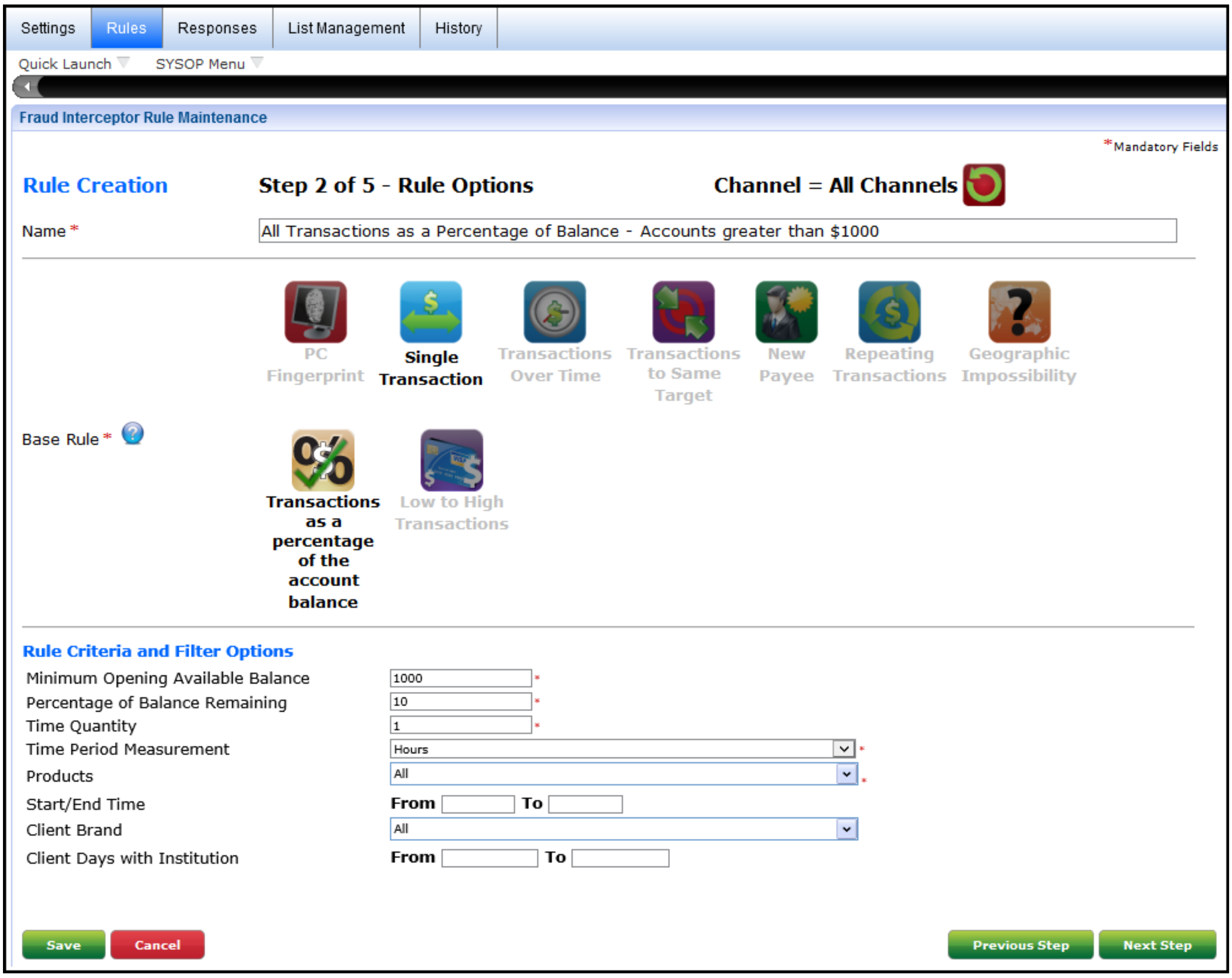


Name * All Transactions as a Percentage of Balance - Accounts greater than $1000

Comments This rule is triggered by a single transaction greater than the specified percentage of the account opening balance.

This rule uses All Channels.

Fraud Interceptor Rule Maintenance - Step 2 of 5 - Rule Options



Step 2 of 5 - Rule Options

Channel = All Channels

Name * All Transactions as a Percentage of Balance - Accounts greater than $1000

Base Rule * Transactions as a percentage of the account balance

Rule Criteria and Filter Options

Minimum Opening Available Balance	1000 *
Percentage of Balance Remaining	10 *
Time Quantity	1 *
Time Period Measurement	Hours *
Products	All *
Start/End Time	From To
Client Brand	All
Client Days with Institution	From To

This rule uses the Base Rule 'Transactions as a percentage of the account balance'.

The following criteria and filter options have been specified:

Minimum Opening Available Balance	This is the minimum available balance of the account at the beginning of the time period being tested.
Percentage of Balance Remaining	This is the percentage of the original balance (Minimum Opening Available Balance) that must be retained after the transaction is considered without breaking the rule. See **Examples of when Transactions Will Break the Rule - Percentage of Account Balance**.
Time Quantity **Time Period Measurement**	These two fields are used together and there are multiple variations that may be appropriate. In this example, '1' and 'Hours' have been selected. This is the maximum time period between the two transactions to be considered for triggering this rule.
Products	'All' has been selected; however, if you only have one or two products types for this rule, you could select the individual product types from the drop-down list. By selecting 'All' you will not have to update the rule when new products are created.
Start/End Time	The From and To fields would normally be left blank in this rule.

ClientBrand	This optional field is only displayed if the Multi-branding module is active. From the drop-down list, select one or more (or 'All') brands applicable to this Rule.
Client Days with Institution	You can restrict the Rule to only apply to clients who have been with your financial institution for a certain number of days. This is particularly useful as a precaution for clients who have only joined recently. Enter positive, whole numbers only in the From and To fields with a range of days between 0 and 99999.

Examples of when Transactions Will Break the Rule - Percentage of Account Balance

Scenario 1

	Transaction 1	Transaction 2	Transaction 3
Time	11:00	11:20	11:30
Balance	$1,000.00	$200.00	$150.00
Transaction Value	- $800.00	- $50.00	- $140.00
New Balance	$200.00	$150.00	$10.00

Transaction 1

The original balance is $1,000.00 and there is a transaction for - $800.00. The remaining balance is $200.00 which is more than 10% of the original balance at the beginning of the series of transactions therefore the rule is not triggered.

Transaction 2

At the start of the transaction, the balance is $200.00. This transaction is for - $50.00 which gives a remaining balance of $150.00. The remaining balance is also more than 10% of the balance at the start of this transaction; however, the rule indicates that the original balance must be $1,000.00 so the rule would not have been broken anyway.

The original balance was $1,000.00 and this is within the 1-hour time period. The new balance of $150.00 is more than 10% of the original balance and therefore the rule has not been broken.

Transaction 3

At the start of the transaction, the balance is $150.00. The transaction is for $14.00 which leaves less than 10% of the value of the transaction. As the starting balance was under $1,000.00, the rule is not broken.

The original balance at the start of the 1-hour time period was $1,000.00 and the current balance of $10 is less than 10% of the original balance and the rule is therefore broken when compared to the original balance.

Scenario 2

	Transaction 1	Transaction 2	Transaction 3
Time	11:00	11:30	11:55
Balance	$300.00	$1,000.00	$50.00
Transaction Value	$700.00	- $950.00	-10.00
New Balance	$1,000.00	$50.00	$40.00

Transaction 1

The original balance is $200.00 and there is a credit transaction for $800.00. The remaining balance is now $800.00. As the balance was increased, the rule is not triggered.

Transaction 2

At the start of the transaction, the balance is $1,000.00. This transaction is for - $950.00 which gives a remaining balance of $50.00. The remaining balance is less than 10% of the balance at the start of this transaction and therefore the rule has been broken.