globalpayments

Global Payments Ecommerce
User Guide

Cloud-based solution to integrate payments your way

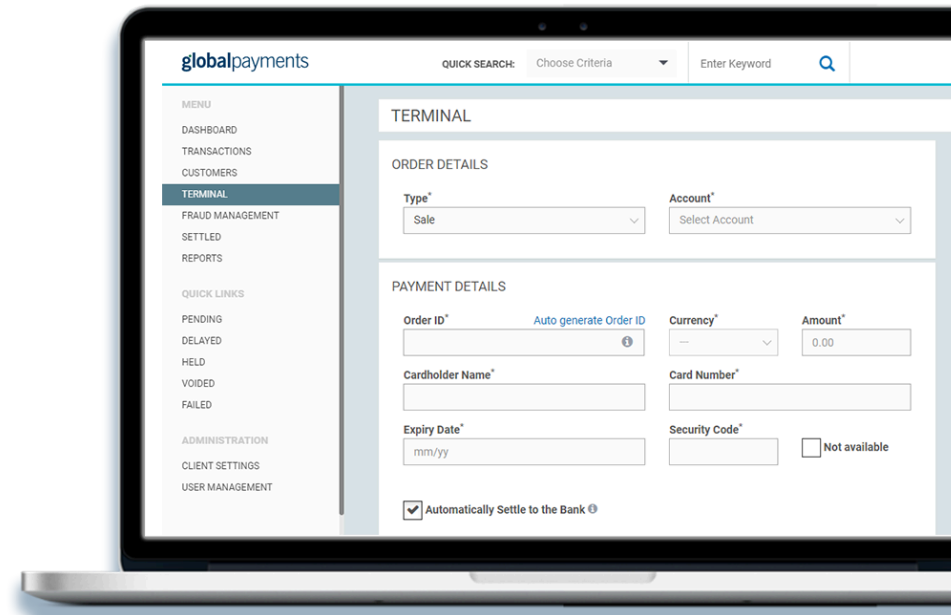# Table of contents

globalpayments

Introduction

Thank you for considering Global Payments as your payment technology solution provider. We offer a wide range of reliable and innovative payment technology solutions that can help your business thrive. With over 50 years of specialized experience serving Canada and a reputation as one of the world's largest and most respected payment technology solution providers, you can trust us to deliver personalized, comprehensive solutions that meet your specific needs.

At Global Payments, we understand that every business is unique, and that's why we take the time to listen to your requirements and craft customized solutions that fit your business perfectly. We're committed to providing you with the best possible support, and that includes a helpful guide to navigating our Ecommerce platform. If you have any questions or need further assistance, our team of experts is always here to help you.

Below are links to the Ecommerce Portal:

- Access your test account:
  https://realcontrol.sandbox.realexpayments.com

- Access your live account:
  https://realcontrol.realexpayments.com

globalpayments

Your account

Learn how to reset your password.

Reset your password

Navigate to the Ecommerce Portal webpage at:
https://realcontrol.realexpayments.com/

1. Click '**Forgot Password**' on the login screen.

2. Enter your details:
   - Client ID - The client ID of the account can be found in your Welcome Email.
   - Username - The username you log in with and set up when registering.
   - Email - Your email address the account is registered with.

3. Depending on your password reset preferences (which can be updated via the **User Management** section in the Ecommerce Portal), you will either receive a password reset email or a password reset email with accompanying verification code. The code will be sent via SMS text message to the mobile phone number you have registered with your account. To navigate to the Password Reset section, go to the '**User Management**' section in your Ecommerce Portal, find the user and click on the dropdown arrow. Then click '**Edit User**'.

4. Once you receive the password reset email from Global Payments, click on the 'Reset My Password' button. The route to reset passwords varies depending on the verification mode that was set up for your account. Follow the section below to complete resetting your password.

Email only	Email and verification code
globalpayments PASSWORD RESET Hi _____ You have requested to reset your password. **RESET MY PASSWORD** *This link will be valid for 24 hours* If you did not request for your password to be reset please email support@globalpay.com to let us know. Kind regards, **Global Payments Support Team** *Global Payments 2018*	**globalpayments** PASSWORD RESET Hi _____ You have requested to reset your password. **RESET MY PASSWORD** *This link will be valid for 24 hours* **You will also receive a text message** *(on the mobile registered with the Ecommerce Portal)* **with your password reset code.** If you did not request for your password to be reset please email support@globalpay.com to let us know. Kind regards, **Global Payments Support Team** *Global Payments 2018*

Email-only verification mode

If you are set up for **email-only password reset**, you will be redirected to the below screen. Create a new password and re-type this password to confirm.
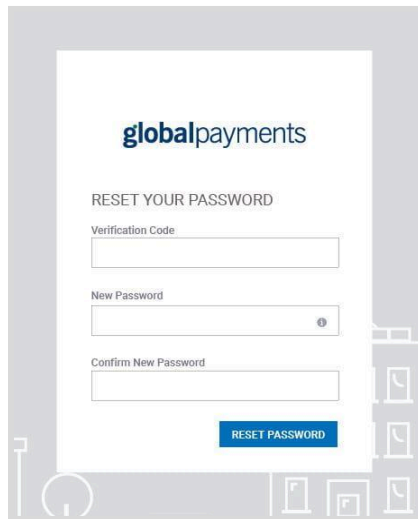
- Uppercase letter(s)
- Lowercase letter(s)
- Number(s)
- Symbols(s) e.g. ! * & % @ _ - + =

Email and Verification Code verification mode

If you are set up for **email and verification code password reset**, you will be redirected to the below screen.

You will receive a **6-digit verification code** via text message. Enter the code, then create a new password and re-type this password to confirm. Click 'Reset Password', and log in with your new password.

globalpayments

RESET YOUR PASSWORD

Verification Code

New Password

Confirm New Password

RESET PASSWORD

Password criteria

To successfully reset your password, the password needs to follow the below criteria:

1. No re-using a previously used password

2. Passwords are case sensitive

3. Passwords must contain at least 10 characters

4. Passwords must contain at least 3 of the following:

globalpayments

User management

Learn how to add new users, set roles and permissions, and view and edit existing users. Find out more about the user registration process in this section.

Access user management

To access user management, you will require the **'Administrator'** or **'User Manager'** role assigned to your **User Login**. These roles are explained in more detail in the **'Setting user Roles and Permissions'** section of this guide.

The '**User Management**' is located under '**Administration**' within the navigation menu.
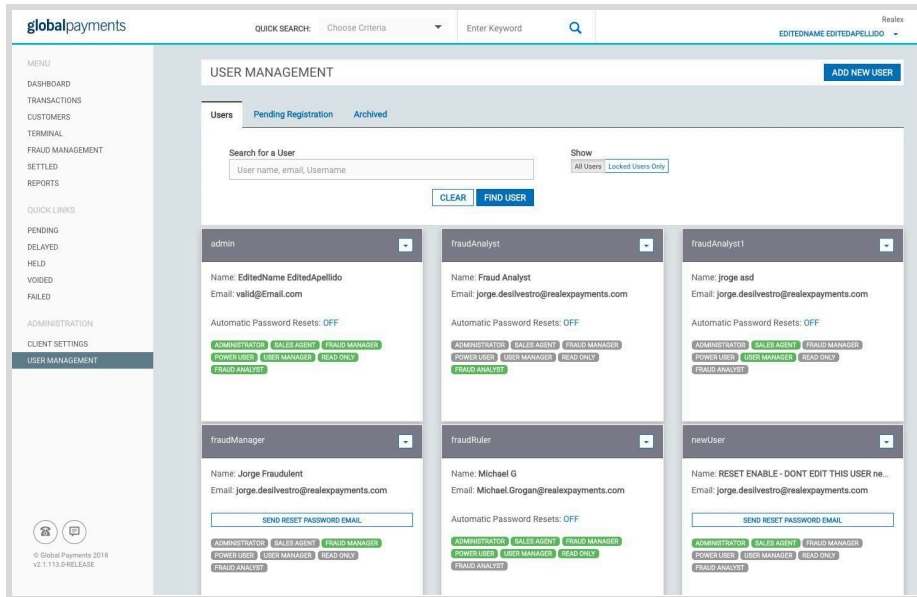
Add new users

1. To create a new **User**, click on '**Add New User**' on the '**User Management**' screen.

2. On the '**Add User**' screen, you can add the '**Automatic Password Reset**' functionality to the user's role by checking the tick box option.

   This functionality allows the user to reset their password automatically anytime they wish.

3. You only need to provide the user's email for setup.

   The Username, first name, and last name are optional and can be set by the user during the registration process.

4. Choose the user role within the **'Roles'** section. The user roles detailed are explained on the '**Add User**' screen.

   For more information on user roles please see the **'Setting user Roles and Permissions'** section of this guide.
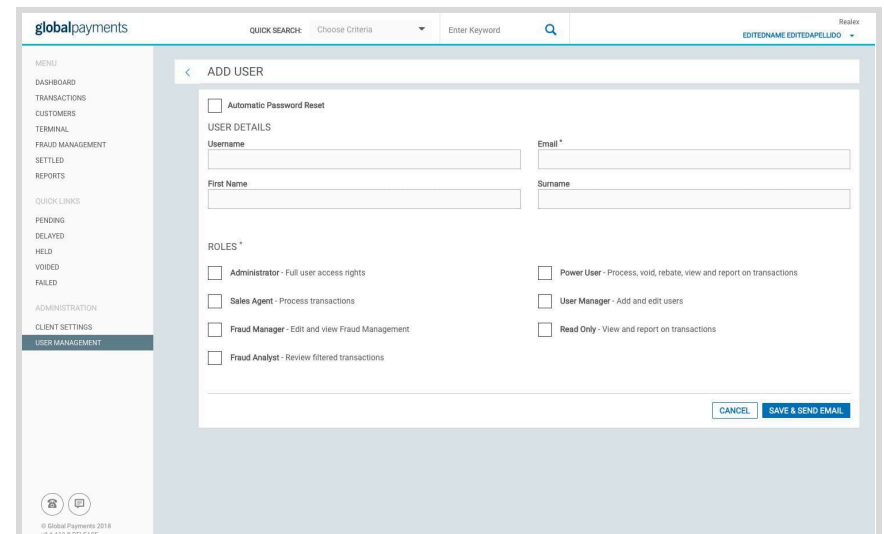
globalpayments

Set user roles and permissions

Users of Global Payments Ecommerce can be assigned multiple roles which define the areas and functionality to which they have access. The following roles can be assigned:
- Administrator
- Power User
- Sales Agent
- Read Only
- Fraud Manager
- User Manager

The table below details the functionality within each user role:

Action	Administrator	Power User	Sales Agent	Read Only	Fraud Manager	User Manager
View transaction details	✓	✓	X	✓	X	X
Generate, view and download reports	✓	✓	X	✓	X	X
Process sales	✓	✓	✓	X	X	X
Perform refunds	✓	✓	X	X	X	X
Perform rebate / void / settle transactions	✓	✓	X	X	X	X
View the settings general section	✓	X	X	X	X	X
Change your existing password	✓	✓	✓	✓	✓	✓
Add new RealControl users	✓	X	X	X	X	✓
Change the roles of other Users	✓	X	X	X	X	✓
Request an Automated Password Reset for other Users	✓	X	X	X	X	X
View the Fraud Management section – View/Edit Rules	✓	X	X	X	✓	X

Note:

All users must be assigned <u>at least one role</u>. Assigning multiple roles will cumulate the possible actions for the user. User managers cannot cumulate multiple roles.

User registration process

Once a user is created, a registration email will be sent to the user's email address. Users will receive an email from **register.reporting@globalpay.com**

Simply click on the registration link in the email to access the registration page as demonstrated on the right.

Enter the fields to complete user registration.

globalpayments

View and edit existing users

In the '**User Management**' screen, you can search for users that you wish to view and/or edit by entering their username, name or email address in the '**Search for a User**' field.

1. The **'Users'** tab will show all registered users in your application.

2. The '**Pending Registration**' tab will show users who have yet to register on the application and the '**Archived**' tab will show users who have had their user access revoked.

   Archived users can be re-activated on the application if needed.

3. You will also have the option to view '**All Users**' or to view '**Locked Users Only**'.
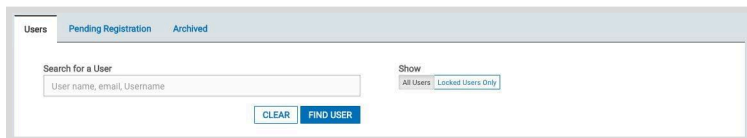
4. To edit a user, click on the dropdown box located on the user's details. Click on the '**Edit**' option as shown below.
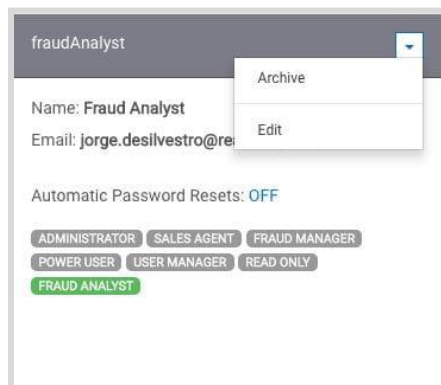
5. Once you have clicked '**Edit**', the below screen will appear:
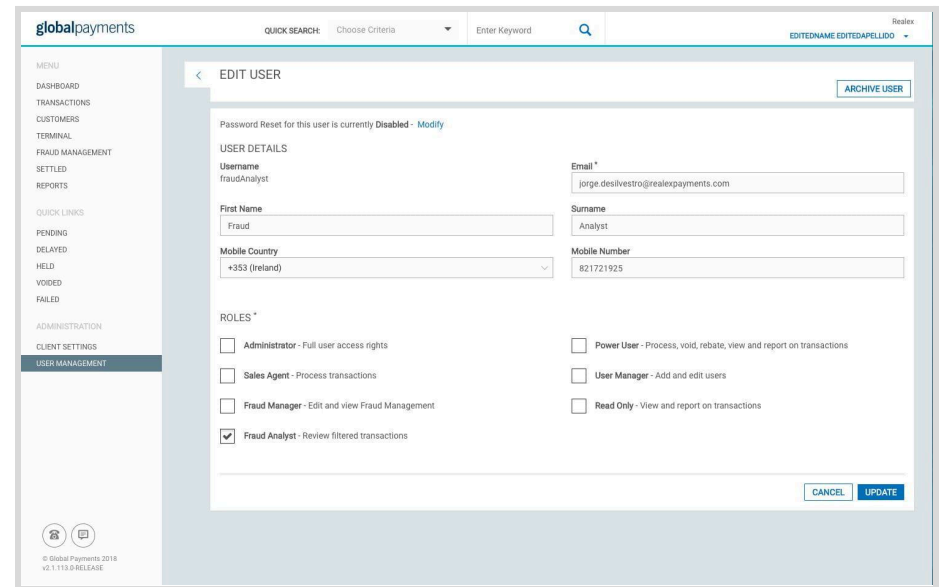
If the user has been set up for automated password resets you will have the option to '**Send Password Reset Email**'. This option allows you to send an email to the user's registered email address containing a link to reset their password.

globalpayments

Processing transactions

To process a transaction in the Global Payments Ecommerce Portal, go to the 'Terminal' section to access the Virtual Teminal function. This section can be found within the navigation menu to the left of the dashboard.

This **Virtual Terminal** function can be used to process card transactions including the following. Click to navigate to the corresponding guides

- **Sales**
- **Refund**
- **Card verification**

Sales

To process a sale on the Virtual Terminal, follow the steps below:

1. In the '**Type**' field, choose '**Sale**' from the dropdown menu.

2. To select a particular sub-account to process the transaction against, choose the '**Account**' from the dropdown menu.

3. If the card you are processing does not have a Security Code, simply tick '**Not Available**' and the related input field will be disabled.

4. If you want to process a pre-authorization (holding funds on a customer's card without immediately capturing them), uncheck the '**Automatically settle to the bank**' tickbox.

5. All fields marked with an ***** are mandatory and must be completed to process the transaction.

6. Once all mandatory fields are complete, click on '**Process**'.

7. The transaction result will display and the appropriate message will appear at the top of the **Terminal** screen.

Refund

To process a refund, you will need to have been assigned the role of '**Administrator**' or '**Power User**' to gain access to this section of the Virtual Terminal.

1. Select '**Refund**' from the '**Type**' dropdown.

2. To select a particular sub-account, choose the sub-account from the '**Account**' dropdown.

3. All fields marked with an ***** are mandatory and must be completed to process the transaction.

   You will be required to enter your login password as this is a mandatory field.

4. Once all mandatory fields are complete, click on '**Process**'. The transaction result will display and the appropriate message will appear at the top of the '**Terminal**' screen as seen in the Sale section above.

Note:

Please note that the refund option is not enabled by default on your account. For more information on this please contact the **Global Payments Support Team**.

You will need the full card number and expiry date to process a refund. If you do not have these details and the transaction is less than 180 days old, you should process a '**Rebate**'. For more information on rebates, please navigate to the **Rebating a Transaction** section of this guide.

Card verification

The card verification transaction type is used to check that a card is valid and active without authorizing or holding funds.

1. To process a card verification transaction, select '**Card Verification**' from the '**Type**' dropdown.

2. To select a particular sub-account, choose the sub-account from the '**Account**' dropdown.

3. All fields marked with an ***** are mandatory and must be completed to process the transaction.

4. Once all mandatory fields are complete, click on '**Process**'.

5. The transaction result will display and the appropriate message will appear at the top of the '**Terminal**' screen as seen in the **Sale** section above.

globalpayments

Surcharging

Surcharging allows you to recoup your transaction processing costs.

Please note that not all Merchant Category Codes (MCC), products and card types are eligible for surcharging. You should validate if your MCC and products are eligible for surcharging.

Please note that Canadian regulations only allow surcharging on credit cards. The province of Quebec does not allow surcharging.

Surcharging needs to be enabled on your merchant account by our support team. You will then be able to configure it to the percentage you are allowed to surcharge (cannot be more than your processing costs).

1. To configure the Surcharge functionality, go to the '**Client Settings**' section and click on the '**Surcharge**' tab.

2. Select the account you need to configure by clicking on the check box next to the account name.

3. Once selected, a new section will let you configure the surcharge rate (percentage only in Canada) you want to apply.

4. Click the '**APPLY SURCHARGE**' button to save the configuration.

5. The screen will now show the configured surcharge rate.

Repeat steps 2 to 4 for each account you need to configure for surcharging.

To process a transaction with a surcharge, go to the '**Terminal**' section and process a transaction as usual. See the '**Processing Transactions**' section for more details.

Once the card number is provided, the terminal identifies if the card is eligible for a surcharge and applies the surcharge rate configured.

Important note: If a card is eligible for surcharging, the customer needs to be informed of the surcharge amount and consent to it. The agent processing the transaction needs to fill the checkbox indicating that the customer was informed and consented to the surcharge.
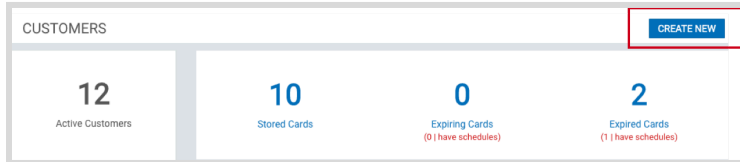
To disable the surcharging while processing a transaction, uncheck the '**Apply surcharge**' checkbox.

globalpayments

Customer management

Learn how to add new customers, add new payment methods and take payments from a saved customer.

Add a new customer

To create a new customer profile, click '**Create New**' and input the customer's details.

The '**Customer Ref**' is used to identify the customer's profile and must be unique. All fields marked with ***** are mandatory.

Click on **'Create Customer'** to save the customer profile.

Once the customer profile has been created, you can add the customer's card details for making future payments.

Add a new payment method

To add a card, click the '**Add Payment Method**' button.

Once you have added the card details click '**Save Payment Method**' to update the customer's profile.

The card details are now securely stored. You can now process a payment against the customer by clicking '**Take Payment**'.

Set up recurring payments

To set up a scheduled recurring payment, click on '**More**' and choose '**New Schedule**' from the dropdown menu.

Set up the schedule to run at the required date and frequency.

All fields marked with the ***** are mandatory.

Click '**Save**' to save the schedule.

The customer profile is now updated with the recurring payment schedule.

globalpayments

Transaction management

Learn how to view, void, rebate, and settle delayed transactions.

View transactions

To view transactions, click on '**Transactions**', located within the main navigation menu.

In the '**Transactions**' section, you can search for multiple transaction types that have been processed.

1. Enter the relevant transaction data in the fields located in the '**Search for Transactions**' section.

2. Within the '**Status'** dropdown, you have the option to filter out specific transaction types.

   For example, if you would only like to view 'Pending' transactions, choose the 'Pending' option from the dropdown and this will return all transactions that match these criteria.

3. The status of the transaction will appear to the right of the transaction line.

   For example, the sample screen below shows all transactions which were processed on February,3rd, 2015 based on the search criteria entered.

4. To view more details on the transaction, click on the transaction line.

Note: Transactions processed with Installments can be filtered by checking the '**Transactions with Installments**' checkbox.

globalpayments

The '**Transaction Details**' screen can also display **installment plan** details, such as:
- Frequency
- Installment Payment Amount
- Total Fees (APR: %)
- Total Including Fees
- Terms And Conditions (including Additional terms hyperlink)

Void transactions

'**Pending**' and '**Delayed**' transaction types can be voided to prevent the transactions from proceeding to settlement. You can search for '**Pending**' or '**Delayed**' transaction types within the '**Transactions**' section.

To '**Void**' a transaction, click on the drop-down box located to the right of the transaction status. Once you have clicked on the drop down you will have the option to '**Void**' as shown below.

You can optionally add comments relating to the transaction in the '**Comments**' section.

Should you wish to view the transaction details before voiding a transaction you can click on the transaction line. This will bring you to the '**Transaction Details**' screen and the '**Void Transaction**' option will be present above the transaction details.

To complete the void, click on the '**Void Transaction**' button. Once a transaction has been voided it will not be sent for settlement.

globalpayments

Rebate transactions

If you need to refund a settled transaction, you'll use the rebate option. Once a transaction has been sent for settlement, it cannot be voided. Instead, to return funds to the customer, you'll process a rebate.

This transaction refunds the cardholder and debits your bank account. Since the rebate utilizes the details from the original authorization transaction, there's no need to contact the customer for their information to process it.

> **Note:**
>
> Rebate can only be accessed if you have sufficient permissions. You will need to have been assigned the role of '**Administrator**' or '**Power User**' to gain access to this section.
>
> To gain access, contact your '**Administrator**' User.

Unlike refunds, rebates come with two specific limitations:

- **Rebate Amount Limit:** You can partially or fully rebate a transaction, or rebate any amount up to 115% of the original authorization.

- **Time Limit:** Rebates can only be processed within 180 days after the transaction's original processing date. After this period, a refund will be necessary. For further details on refunds, please refer to the **Refund** section.

To process a rebate, follow the steps below:

1. Click on the transaction you wish to rebate. At the top of the transaction details screen, click on '**Rebate Transaction**'.
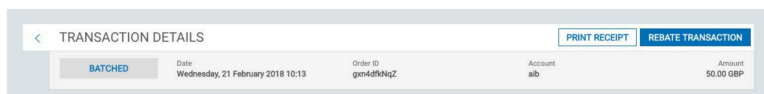
2. The screen below appears, allowing you to enter further details before finalizing the rebate. You can add the rebate '**Amount**', '**Customer Number**', '**Variable Reference'**, '**Product ID**' and any additional comments for reconciliation purposes.

3. Enter your login password to proceed

4. Click on '**Rebate Transaction**' to process this transaction. You can then view the rebated transaction in the '**Transactions**' section.

globalpayments

Settle delayed transactions

To find a delayed settlement transaction, navigate to the '**Transactions**' section. Once there, use the search function to locate delayed transactions. Select '**Delayed**' from the '**Status**' field and click '**Search**' to view all delayed transactions that match your criteria.

Once you've found the transaction you want to settle, click on it and choose the option '**Settle Transaction**'.

To add additional information relating to the transaction, go to the '**Settle**' screen as shown below.

Click on '**Settle Transaction**' to process this transaction. You can then view this transaction within the '**Pending**' category.

Transaction reporting

Learn more about batched transactions, viewing related transactions, printing receipts, and downloading reports as an Excel file.

Batched transactions

Once transactions are authorized, they are forwarded to the acquiring bank for settlement at the end of each day (midnight merchant local time). At this point, the transactions become settled transactions and are grouped into daily batches for processing.
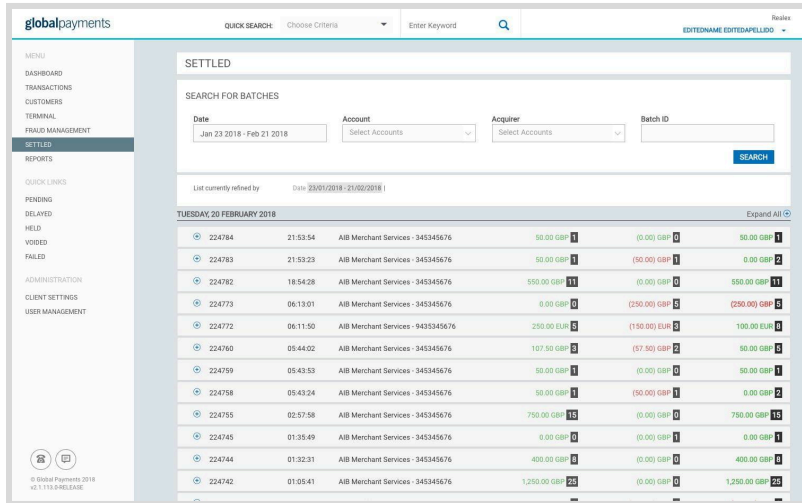
Note:

While batches are closed daily by Global Payments, banks only fund merchant accounts Monday to Friday.

Batch overview

To view settled transactions in batches, click on 'Settled' from the navigation menu on the left side of the screen.

All settled transactions are grouped under a daily batch ID.

To view further information on the batch of settled transactions click on the batch line. The 'Batch Overview' screen will then be displayed:
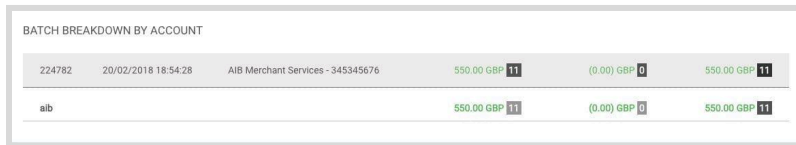
If you wish to generate a report based on the transactions within that batch, click on 'Generate Report'.

To view all transactions within the batch, click on 'View Transactions', and you will see the screen below.
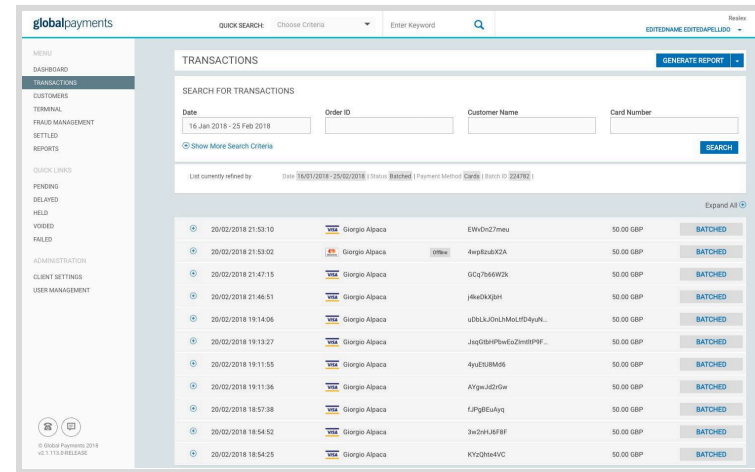
To view more details about a transaction, simply click the plus (+) sign located on the left of the transaction line. This will expand the transaction line and provide additional information. Alternatively, you can click on 'Expand All' to view extra details for all transactions in the batch at once. Clicking on each transaction line allows you to access individual transaction details. In the transaction details section, you'll find general information about the transaction.

globalpayments
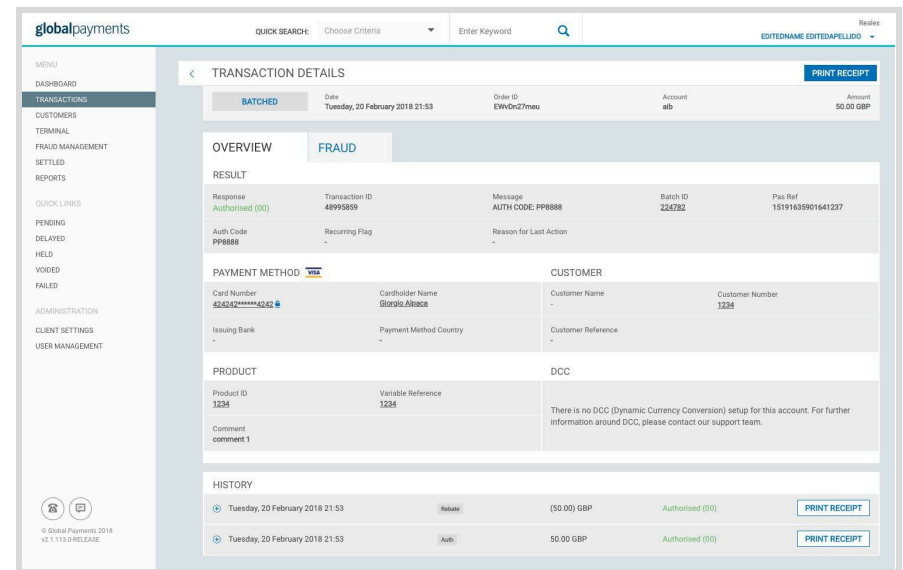
Fraud

In the fraud section of the transaction details screen, you can view the **Fraud Score**, **Security Code** and **3D Secure information**. You can also view the **AVS Address** and **AVS Postcode** results returned for the transaction.

Explanation of details within the **Fraud** section of transaction details:

Title	Description
UCAF (AAV/CAVV)	This is the Cardholder Authentication Verification Value created during cardholder authentication.
XID	This is a Global Payments generated transaction reference that the merchant sends to the Access Control Server in advance of the cardholder authentication.
ACS URL	This is the address of the Access Control Server, the card issuing banks website.
ECI	This is the E-Commerce Indicator. For more information on this field, please see the below table.

Visa	Mastercard / Switch (UK DMK)	Ecommerce Indicator (ECI)
5	2	Full 3D Secure – cardholder Enrolled and authenticated
6	1	Merchant 3D Secure – cardholder not enrolled or attempt to contact ACS server was used
7	0	Non 3D Secure transaction.. It is up to the merchant to decide whether or not to proceed with a non-3D Secure transaction. The liability shift no longer applies.

Note that transactions processed on the Virtual Terminal cannot benefit from the 3D Secure liability shift. Only customer-initiated ecommerce transactions can benefit from 3D Secure.

Transaction history

In the history section of the transaction details screen, you can view the details of the authorization and all subsequent actions that have been carried out against the order. These may include settle, rebate, and void details.

Explanation of fields on transaction details screen:

Field	Description
Timestamp	The date and time the transaction was processed.
Cardholder Name	The Cardholder name.
Order ID	This is the unique identifier for the transaction.
Account	The sub-account that the transaction was processed under.
Transaction Amount	The value of the transaction.
Customer Number	This displays information sent in the Customer Number field of the authorisation.
Product ID	This displays information sent in the Product ID field of the authorisation.
Variable Reference	This displays information from the Variable Reference field.
Status	This shows the current stage of the transaction process.
Result	The result of the transaction which is passed back by the card holders issuing bank.
Message	This is the result message which is passed back by the card holders issuing bank.
Batch ID	This shows the Batch ID of the batch that the transaction is associated with. If a transaction is declined and therefore not batched, this will display '-1'. In this instance the Batch ID will be available in the 'Settled' section of the application.
Pas Ref	This is an internal Global Payments reference, unique to each transaction.
Transaction ID	This is an internal Global Payments reference, unique to each transaction.
Card Number	This shows the card type and the card number masked with X's for security reasons. The first 6 digits and last 4 digits will be the only characters visible.
Card Issuer	This displays the name of the bank that issued the card, if that information is available.
Card Issuer Country	The country the card was issued in.

globalpayments

Originating I.P.	This shows the IP address that the transaction was processed through.
Customer I.P.	This shows the IP address of the customer.
Fraud Score (TSS)	This is the score that the transaction received by the fraud scoring tool.
Security Code	This shows the result of the Security Code check. Please see the Appendix for the possible security code results.
AVS Address	This shows the result of the Address Verification Service (AVS) check on the information supplied by the customer in the billing address field.
AVS Postcode	This shows the result of the Address Verification Service (AVS) on the postcode supplied by the customer.

View related transactions

In the '**Payment Method**' section of the transaction details screen you can view related transactions by clicking on **Number** or **Cardholder Name**. These values will be underlined as below.

For example, if you click on the card number this will display all transactions processed on this card.

PAYMENT METHOD **VISA**

Card Number
424242******4242

Cardholder Name
Giorgio Alpaca

Issuing Bank
-

Payment Method Country
-
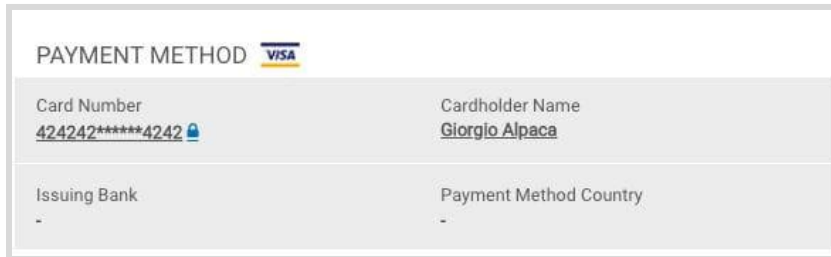
View and print receipt

To print a receipt, click on the '**Print Receipt**' button which will appear on the top right of your transaction details screen. This will open up a new tab in your browser, containing the receipt. Then use the onscreen options to save or print the receipt as necessary.

< TRANSACTION DETAILS   PRINT RECEIPT

BATCHED	Date	Order ID	Account	Amount
	Tuesday, 20 February 2018 21:53	EWvDn27meu	aib	50.00 GBP
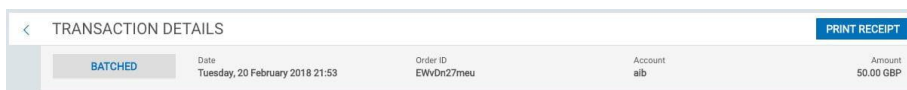
Download reports to Excel

To generate reports of all transactions, click on '**Generate Report**'.

For example, within the 'Settled' section, the 'Generate Report' button is located within the batch overview screen below.

This will produce a report of all transactions within that batch. This functionality can be used throughout multiple sections of the RealControl system wherever the '**Generate Report**' button is located.

Click on '**Generate Report**', this will schedule the batch report in the '**Reports**' section of the application.

BATCH 224782 OVERVIEW   GENERATE REPORT ▾   VIEW TRANSACTIONS

BATCH BREAKDOWN BY ACCOUNT

224782	20/02/2018 18:54:28	AIB Merchant Services - 345345676	550.00 GBP 11	(0.00) GBP 0	550.00 GBP 11
aib			550.00 GBP 11	(0.00) GBP 0	550.00 GBP 11

To view reports click on the '**Reports**' section of the main navigation menu. Click the '**Download**' icon to the right of the report line to open or save the file. If you choose to save the file, you can save it as a **.csv** file on your local device.

globalpayments

Fraud management guide

Discover how to establish rules, input transaction data, and manage suspicious transactions by reviewing, releasing, or voiding them. Learn methods to block, hold, or restrict transactions, and more.

While selling online offers vast opportunities for business growth and scalability, it also comes with inherent fraud risks. These risks can be mitigated by:

- Implementing 3D Secure for all online transactions. This practice shifts the majority of fraud liability from you to your customer or their bank. Many acquiring banks mandate the use of 3D Secure for online transactions.

- Verifying the Security Code and Address Verification (AVS) results for transactions. Ensure accurate data submission and proper interpretation of these results to enhance security measures.

- Global Payments Fraud Management for automated transaction handling, including passing, holding, or blocking transactions based on predefined rules and criteria.

What rules can I set up to get started with Fraud management?

This guide provides a recommended set of Fraud Management rules for new merchants with limited online selling and fraud management experience. Configuring these rules adds an extra layer of protection beyond 3D Secure, Security Code, and AVS, while also enhancing your understanding of the Global Payments Fraud Management product. This knowledge empowers you to customize the rules to align with your specific business requirements effectively.

Note:

This guide is a recommendation only. You must take ownership of your own Fraud Management rules. Take a look at the other available rules to see if you feel any other rules would help you mitigate fraud.

Fraud Management Rule Creation

Fraud Management is a Global Payments product that executes a series of rules, configured by you, at the time the transaction is authorized that can PASS, HOLD or BLOCK transactions automatically. It helps you identify suspected fraudulent transactions. It may be difficult for you to know what rules to configure before you commence processing online transactions for the first time, so here are some recommendations to get started with.

Please note that all the recommended rules result in a HOLD or PASS result. **These rules will not automatically BLOCK transactions.** Using HOLD ensures you never lose a sale automatically. A PASS result means the transaction is accepted, while BLOCK means that the transaction is stopped and will never be processed. A HOLD result means that if the transaction is authorized, you will not receive funds for that transaction until the transaction is reviewed and released by you. Please do not ship goods until a held transaction is reviewed by you and released.

If you are uncomfortable with Fraud Management automatically holding transactions that you subsequently need to review, you can set Fraud Management to PASSIVE MODE. Passive mode means that the Fraud Management result is for information only and no automatic action, such as holding the transaction, is taken. See 'What are PASSIVE and OFF modes used for?' section later in this document.

Below are 7 rules we would recommend that you enable before you start processing transactions.

To configure these rules log in to RealControl and go to Fraud Management → Create A New Rule.

You can give each rule a name that means something to you. Your rule names appear in RealControl when you view detailed information about a transaction.

Amount

> *'I want to hold transactions when the amount is greater than £x. Otherwise, I want to pass transactions.'*

You need to determine the amount, once exceeded, for which transactions will be held. We recommend looking at your average sale amount and then choose a larger amount where, if seen, you would want to review before accepting.

Customer

> *'I want to hold transactions when the cardholder name is marked as medium risk in my cardholder name data list. Otherwise I want to pass transactions.'*

You need to add cardholder names to your data list as Medium risk for this rule to trigger. It's unlikely you will have any cardholder names when you first start processing transactions. Over time you can easily add names from previous transactions via RealControl. This should be done if you ever get a transaction that results in a fraud chargeback.

See '**How do I block/hold transactions based on the data in my data list?**' within the Fraud Management Guide section.

Geographic

> *'I want to pass transactions when the issuer country is marked as low risk in my issuer country data list. Otherwise I want to hold transactions.'*

You will need to add countries to your payment method country list that you want to accept.

See '**How do I restrict transactions to a set list of countries?'** within the Fraud Management Guide. Alternatively, you can reverse this rule to HOLD transactions for a known list of countries and PASS for all other countries.

Please note that holding transactions where the Billing and Shipping Countries or Billing and Issuing Countries do not match is also popular. To use these rules please ensure you are submitting Shipping and Billing Countries to Global Payments in your transactions.

Card Number

> *'I want to hold transactions when the card number has been used more than x times with a different cardholder name. Otherwise I want to pass transactions.'*

You need to replace x with a number indicating how many times you are comfortable with a card number being used with a different name before you want to hold the transaction for review

See '**How do I block/hold transactions based on a particular pattern?**' within the Fraud Management Guide.

> *'I want to hold transactions when the card number is marked as medium risk in my card number data list. Otherwise I want to pass transactions.'*

globalpayments

You need to add card numbers to your data list as Medium risk for this rule to trigger. It's unlikely you will have any card numbers when you first start processing transactions but over time you can add them securely from previous transactions via RealControl, especially if you ever get a chargeback.

See '**How do I block/hold transactions based on the data in my data list?**' within the Fraud Management Guide.

> *'I want to hold transactions when the card number has been authorized more than x times in the last 24 hours. Otherwise I want to pass transactions.'*

> *'I want to hold transactions when the card number has been authorized more than x times in the last week. Otherwise I want to pass transactions.'*

You need to decide how many times you want to see a card number authorized in the past 24 hours and in the past week, before holding it.

See 'How do I block/hold transactions based on recurrent use of a card number within a defined period?' Fraud Management Guide.

The above rules are a recommendation only. Enabling these rules will give you a good sense of how to use Fraud Management. You can easily configure additional rules based on the data you send to Global Payments. For example, if you are submitting a customer number unique to your business, customer IP address or email address you can build useful rules relating to this data.

Full list of fraud rules

'I want to Pass/Hold or Block transactions when ...'

All categories	...the data list data* is marked as high/medium/low risk
Card number	...the card number has been used more than a number of times in the last 24 hours ...the card number has been authorized more than a number of times in the last 24 hours ...the card number has been used more than a number of times in the last week ...the card number has been used more than a number of times with a different cardholder name ...the card number has been used more than a number of times with a different customer number ...the card number has been used more than a number of times with a different variable reference ...the card number has been authorized more than a number of times in the last week ...the card number has been authorized more than a number of times with a different cardholder name ...the card number has been authorized more than a number of times with a different customer number ...the card number has been authorized more than a number of times with a different variable reference
Geographic	...the shipping and the billing country is different or the same or missing one information ...the shipping and the issuing country is different or the same or missing one information ...the shipping and the home country is different or the same or missing one information
Amount	...the amount in a currency is greater than an amount
Customer	...the cardholder name has been used more than a number of times with a different card number ...the customer number has been used more than a number of times with a different card number
Product	...the variable reference has been used more than a number of times with a different card number
Third party	...the Decision Manager response is (accept/reject/review/error).

globalpayments

* The data list allows you to specify values that should trigger an action should they appear within a particular transaction field. The fields for which data can be listed are:

Card number	Shipping Area
Cardholder name	Shipping Country
Product ID	Billing Area
Variable Reference	Billing Country
Customer Number	BIN range
Customer IP Address	Issuing Country

How to log in and create a new rule?

1. Access the Fraud Management Page by clicking on '**Fraud Management**' on the left-hand side menu and clicking the **Create New Rule** button.

Note:

You must have sufficient privileges to access this functionality. You must be a Fraud Manager or an Administrator. Fraud Analysts can review and manage Fraud Filter transactions but not change rules.

Select the relevant category.

2. Give the rule a name. This is a name that will be re-used throughout the application. In our example type in 'card-holder name and card number'.

Create statement - each rule is made up of one or more statements, and each statement has an action and one or more conditions.

globalpayments

3. Click the Review and Activate button. Review the rule that you have just created and edit or activate it.

It is important to note that activating, deleting or editing Fraud Filter Rules, will result in a change to the transaction response that is returned by Global Payments to your system, either via **API** or via the **Hosted Payment Page**. Please ensure your system is capable of handling changes to the Fraud Filter response from Global Payments to prevent any impact to your transaction processing.

What do I do once I have my rules configured?

Firstly, send in a few test transactions to trigger the rules you have set up to hold the transactions. Then look at those test transactions in RealControl and understand how to review, release and void transactions.

When you start processing real transactions you must monitor them in RealControl.

Go to the **Fraud Management → Fraud Filter** in RealControl to ensure the transactions that are held are reviewed and either released or voided.

See '**How do I review, release or void a suspected fraudulent transaction?**' within the Fraud Management Guide.

Over time if you feel you are spending too much time reviewing transactions you can tweak the rules to let more transactions PASS or BLOCK automatically.

If you find you are getting fraudulent transactions, for example via the chargeback process, then look at those transactions and identify rules which can be added or modified to Hold or Block similar transactions. Add card numbers, cardholder names or other data from chargeback transactions in RealControl to your fraud data lists. Future transactions with that card number, cardholder name or other data will be actioned automatically once the corresponding rule for that data is active.

For detail, review the sections '**How do I add transaction data to my data list?**' and '**How do I block/hold transactions based on the data in my data list?**' within the Fraud Management Guide.

globalpayments

see the action that would have been taken had your Fraud Filter been in ACTIVE mode.

Once you are confident that your rules are working as expected, you can then switch to ACTIVE mode.

When the **Fraud Filter** is in OFF mode, your rules will not be executed but they will be retained in case you want to change to PASSIVE or ACTIVE mode in the future. For security, you will be required to enter your password to set the Fraud Filter mode to OFF.

How do I switch between modes?

You can access the PASSIVE and OFF mode from the '**More Actions**' button on the top right of the Fraud Dashboard screen.

What are the PASSIVE and OFF modes used for, and how do I switch between modes?

What are the PASSIVE and OFF modes used for?

By default, Global Payments' Fraud Management tool is in ACTIVE mode. This means that as soon as you create your rules, they will be applied to all your transactions and the relevant action will be applied.

PASSIVE mode can be used to test your rules before you use them in ACTIVE mode. When the Fraud Filter is in PASSIVE mode, the rules that you have set up will be applied but the actions associated with them (Pass, Hold or Block) will not be executed. However, you will be able to

globalpayments

PASSIVE Mode Will execute the rules and indicate what action (Pass, Hold or Block) your rules would have taken without actually performing that action.

Password*

CANCEL   SWITCH TO PASSIVE

RULES PASSIVE MODE ⓘ   RULES OFF MODE ⓘ

Note:

The password is your login password.

How do I add transaction data to my data list?

What is a data list?

The data list allows you to specify values that should trigger an action if they appear within a particular transaction field. For example, you can use your data list to block transactions from a particular country or a specific card number.

Note:

You will need to set up a rule to define the action that should take place for a listed value.

The data list includes the following list types:

Card number	Shipping Area
Cardholder name	Shipping Country
Product ID	Billing Area
Variable Reference	Billing Country
Customer Number	BIN range
Customer IP Address	Issuing Country

To modify your data list, first access the Fraud Management Page by clicking on '**Fraud Management**' on the left-hand side menu, and then **Add Data** to the **Data List Panel**. There are two ways to add some data to a data list:

1. From the **Transaction Details** page – This panel shows the data collected from this transaction. You can review that data and add or edit its risk by clicking on '**add**' or '**edit**'.

2. From the **Data List** tab – If you know the data that you want to add, select the '**Data List**' tab from the **Fraud Filter** screen and

globalpayments

select the relevant list type. On the list type page, input the data that you want to add to the list. If that data does not already exist in this list type, it will be added straight away. You must assign a level of risk to the item (low, medium or high). If the data already exists, it will be highlighted in the list and you can edit its risk level if required.

How do I block/hold transactions based on the data in my data list?

Note:

Instruction here assumes that you have already added a card number to your data list. Please see the user guide 'How do I add transaction data to my data list?' for more information.

1. Access the Fraud Management Page by clicking on '**Fraud Management**' on the left hand side menu.

2. **Add Data** to **Data List Panel**

3. Create a new rule by clicking the '**Create A New Rule**' button on the Fraud Management Dashboard screen.

globalpayments

4. Select the relevant category, for example, '**Card Number**'.

5. Give the rule a name. This is a name that will be re-used throughout the application. In our example type in '**Card number data list**'.

6. Create your statements. Each rule is made up of one or more statements, and each statement has an action and one or more conditions.

In this case:

> *I want to block transactions (action)*
> *When the card number is marked as high-risk (condition)*

You can add another condition by clicking on the plus icon.

For example, if you also want to block the transaction when the card number is marked as medium risk, you can add the condition:

> *When the card number is marked as medium risk*

You can add another statement to the rule by clicking on the button. For example:

globalpayments

7. Click on the '**Review and Activate**' button.

8. Review the rule that you have just created and edit or activate it.

It is important to note that activating, deleting or editing **Fraud Filter Rules**, will result in a change to the transaction response that is returned by Global Payments to your system, either via XML or via the Hosted Payment Page.

Please ensure your system is capable of handling changes to the Fraud Filter response from Global Payments to prevent any impact to your transaction processing. For full details of the changes see the Fraud Management Developer Guides.

How do I review, release or void suspected fraudulent transactions?

1. Access the Fraud Management Page by clicking on '**Fraud Management**' on the left hand side menu.

2. Access the Fraud Filter screen. The first part of this screen gives you an overview of the transactions that have been recently held or blocked and their overall value. To access the Fraud Filter page, click on the link '**View All Fraud Filter Transactions**'

3. Review, Void or Release from the **Fraud Filter > List of all transactions held or blocked**.

This screen shows the list of all the transactions that were held or blocked by the Fraud Filter tool as a result of the rules that you have in place.

- The '**Held**' transactions for the last 30 days will be listed. To remove a transaction from this list, you must release or void it. You can do this directly from the Fraud Filter Transaction list or on the individual Transaction Details screen.
- The '**Blocked**' transactions from the last seven days will be listed. You cannot remove these but you can review the transaction details and data from the transaction to your data list.

Held transactions need your attention. You must void or release them.
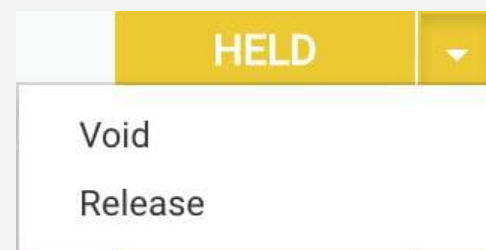
- Failed transactions that were flagged as Held by the Fraud Filter but also failed authorization are listed.
- They do not require any action but you might want to review and add transactional data to the data lists.

4. **Fraud Panel** – In the fraud panel of the Transaction Details screen, you will be able to see the rule (or rules) that caused the transaction to be held or blocked. At the top of the page, you are given the option to release or void the transaction.

How do I block/hold transactions based on a particular pattern?

1. Access the Fraud Management Page by clicking on '**Fraud Management**' on the left hand side menu.

2. Create a new rule by clicking the '**Create A New Rule**' button on the Fraud Management Dashboard Screen.

3. Select the relevant category, in our example select '**Customer**'.

4. Give the rule a name. This is a name that will be re-used throughout the application.

   In our example type in 'card-holder name and card number'.

globalpayments

5. Create your statements. Each rule is made up of one or more statements, and each statement has an action and one or more conditions.

In this case:

> *I want to block transactions (action)*
> *When the card number is marked as high risk (condition)*

For this condition, the number of times the card has been used can be changed if you require it.

You can add another statement to the rule by clicking on the button. For example, for a lesser number of recurrences, you may choose to hold the transaction rather than blocking it:

> *I want to hold transactions when the cardholder name has been used more than 3 times with a different card number.*

In this case, the number of times the card is used should be lower than in the previous statement.

6. Click on the 'Review and Activate' button.

7. Review the rule that you have just created and edit or activate it.

REVIEW AND ACTIVATE NEW RULE

cardholder name and card number   EDIT

I want to block transactions when the cardholder name has been used more than 5 times with a different card number. I want to hold transactions when the cardholder name has been used more than 3 times with a different card number. Otherwise I want to pass transactions.

CANCEL   ACTIVATE RULE

It is important to note that activating, deleting or editing Fraud Filter Rules, will result in a change to the transaction response that is returned by Global Payments to your system, either via XML or via the Hosted Payment Page.

Please ensure your system is capable of handling changes to the Fraud Filter response from Global Payments to prevent any impact to your transaction processing. For full details of the changes see the Fraud Management Developer Guides.

How do I restrict transactions to a set list of countries?

1. Access the Fraud Management Page by clicking on '**Fraud Management**' on the left-hand side menu.
2. Create a new rule by clicking the '**Create A New Rule**' button on the Fraud Management Dashboard Screen.

3. Select the relevant category, in our example select '**Geographic**'.

globalpayments

5. Create your statements. Each rule is made up of one or more statements, and each statement has an action and one or more conditions.

In this case:

> *I want to pass transactions (action)*
> *When the cardholder name has been used more than 5 times with a different card number (condition)*
> *When the issuing country is marked as low risk (condition)*

Set the default statement
The default statement determines what will happen if none of the other statements apply to this rule.

In this case, we would set the default statement to:

> *Otherwise I want to block transactions*

4. Give the rule a name. This is a name that will be re-used throughout the application. In our example type in '**Issuing Country Exclude**'.

6. Click on the '**Review and Activate**' button.

7. Review the rule that you have just created and edit or activate it.

It is important to note that activating, deleting or editing Fraud Filter Rules, will result in a change to the transaction response that is returned by Global Payments to your system, either via XML or via the Hosted Payment Page.
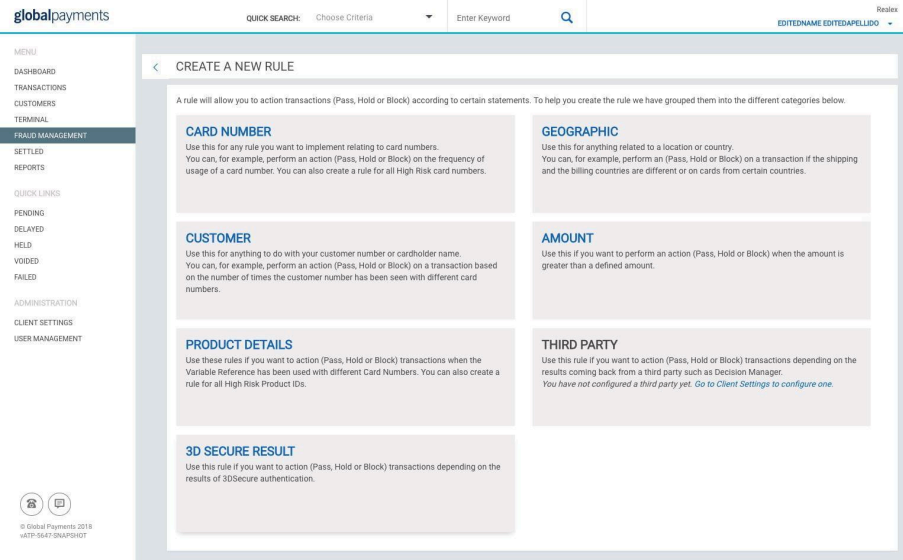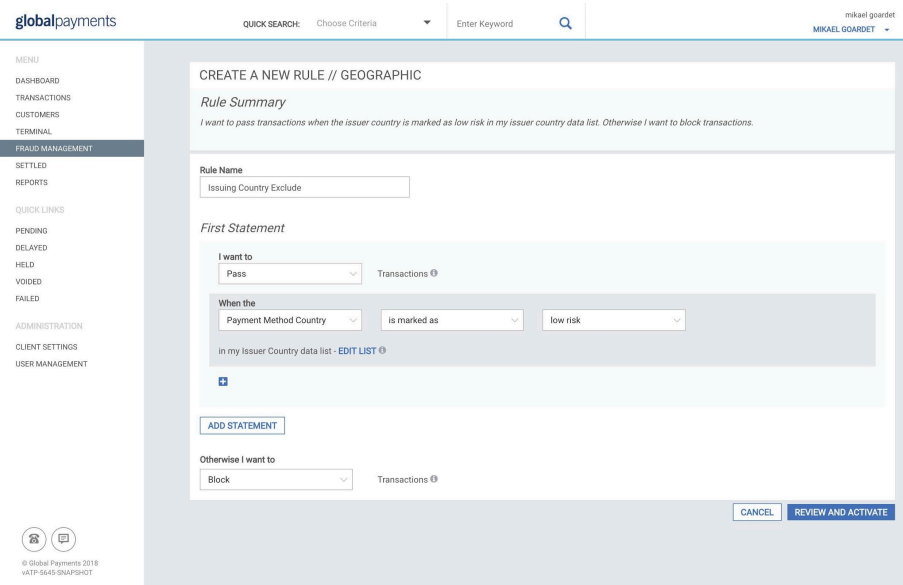
Please ensure your system is capable of handling changes to the Fraud Filter response from Global Payments to prevent any impact to your transaction processing. For full details of the changes see the Fraud Management Developer Guides.

globalpayments

How do I block/hold transactions based on recurrent use of a card number within a defined period?

1. Access the Fraud Management Page by clicking on 'Fraud Management' on the left hand side menu.
2. Create a new rule by clicking the 'Create A New Rule' button on the Fraud Management Dashboard Screen.

3. Select the relevant category, in our example select 'Card Number'.

4. Give the rule a name. This is a name that will be re-used throughout the application. In our example type in '**Card number last 24 hours**'.

5. Create your statements. Each rule is made up of one or more statements, and each statement has an action and one or more conditions.

In this case:

> *I want to pass transactions (action)*
> *When the cardholder name has been used more than 5 times with a different card number (condition)*
> *When the card number has been used more than 5 times in the last 24 hours (condition)*

For this condition, the number of times the card has been used and the time period can be changed if you require.

You can add another statement by clicking on the '**Add Statement**' button For example:

> *I want to hold transactions*
> *When the card number has been used more than 3 times in the last 24 hours*

6. Click on the 'Review and Activate' button.

7. Review the rule that you have just created and edit or activate it.

REVIEW AND ACTIVATE NEW RULE

Card number last 24 hours   EDIT

I want to block transactions when the card number has been used more than 5 times in the last 24 hours. Otherwise I want to pass transactions.

                                        CANCEL   ACTIVATE RULE

It is important to note that activating, deleting or editing Fraud Filter Rules, will result in a change to the transaction response that is returned by Global Payments to your system, either via XML or via the Hosted Payment Page.

Please ensure your system is capable of handling changes to the Fraud Filter response from Global Payments to prevent any impact to your transaction processing. For full details of the changes see the Fraud Management Developer Guides.

Frequently asked questions

What are your office hours?
Monday to Friday, 9.00am to 5.00pm EST

Can I get a receipt for each transaction?
Yes. Transaction receipts are available from our Ecommerce Portal. For details, see the **Transaction reporting section**.

Will you send our customer an email after each transaction?
No. The Ecommerce portal can generate a receipt for you, but does not automatically send the receipt to your customers. You can however download the receipt and send it through your own emailing system.

Do you transfer the money into my business account?
We send the instruction or settlement file to your merchant bank to advise them to debit the customer's card-issuing bank. Your merchant bank is then responsible for the transfer of funds.

How long does it take for funds to settle into my account?
The process of settling funds is handled by your merchant bank. Typically you can expect to receive the funds between 1-5 working days after the authorisation. For more information please contact your merchant bank.

Can I process transactions without a merchant ID?
No. A merchant ID is required to process transactions. Please contact a Global Payments Sales Representative to obtain one.

globalpayments

How do I take payments over the phone?
Our Virtual Terminal and Ecommerce Portal applications allow you to securely accept payments from all major credit and debit cards over the phone. With our Virtual Terminal, you can automatically check the validity of a card and instantly find a historical transaction while on the phone to a customer.

How do I process a rebate?
Rebates can be processed through our Ecommerce Portal application or via remote XML. Simply locate the original transaction in the '**Transactions**' section in Ecommerce Portal. Once located, click '**Rebate Transaction**' button at the top right-hand corner of the screen. You will then be asked for your Ecommerce Portal password to submit the rebate.

My customer has not received their rebate yet. What can I do?
The length of time it takes for a rebate to process depends on the customer's card-issuing bank. In most cases, the customer receives their rebate within 5-10 working days. Some issuing banks may accept rebate receipts from a merchant in an attempt to expedite the settlement process.

Do you provide a plugin for my shopping cart?
We provide plugins for most of the world's leading shopping carts and Ecommerce platforms. We've worked closely with leading developers who are experts in each shopping cart to ensure that every Global Payments plugin is feature-rich and of the highest standard. Our plugins can be found on the respective add-on stores and marketplaces for each cart. Check out our list on **Developer Portal** for more information.

Do I get email notification of failed/declined transactions?
No. When processing transactions on the Virtual Terminal, the transaction result is displayed in real-time in front of you.

I've lost or forgotten my Ecommerce Portal password. How can I reset it?
You can reset your password by clicking the'Forgot Password' link on the Ecommerce Portal login screen.
https://realcontrol.realexpayments.com
For help, download instructions for resetting your password **here**.
Visit the **resetting your password section** of this guide for detailed instructions.

What is 3D Secure?
3D Secure is a customer authentication service introduced by Visa, Mastercard and American Express. The service is individually branded as Verified by Visa, MasterCard SecureCode and Amex Safekey. It is a service designed to protect both the merchant and cardholder from fraudulent e-commerce transactions by adding an extra layer of security for online credit and debit card transactions. Consumers are prompted to enter a personal passcode after their card details have been entered.

What is the URL for Ecommerce Portal?
https://realcontrol.realexpayments.com

Where can I get some test card details? What do I enter for expiry date, name and CVN?
Test card details are available from our **Developer Portal**. You will be required to use any future expiry date, any name and any random 3-digit CVN number to process a test transaction. When testing, please ensure you use our dedicated sandbox environments. Please contact a member of Support at **ca.ecomsupport@globalpay.com** for further information.

Where can I find developer documentation?
All developer documentation and resources are available from our **Developer Portal**.

globalpayments

Call-in support

Contact Global Payments Customer Care Centre at: **1.888.366.5110**
9.00am - 5.00pm EST, Mon - Fri excluding public holidays.

globalpayments