



# Server-to-Server Credit and Debit Card Implementation Guide

---

Merchant implementation instructions to integrate to the Setcom's credit and debit card processing platform. Covers: fraud screening, Verified by Visa, MasterCard SecureCode integration, card authorisation, settlement and refund.

### **Copyright and Trademark**

© 2010 Setcom (Pty) Ltd. All Rights Reserved. Setcom and the Setcom logo are registered trademarks of Setcom (Pty) Ltd. Designated trademarks and brands are the property of their respective owners.

### **Notice of Liability**

The information in this pack is distributed in an “as is” basis. All information provided in this document is provided with good will. The authors and publishers of this manual are not responsible for loss, or purported loss due to any contents of this publication.

## Summary of Revisions

Version	Date	Changed By	Changes Made
2.0.0	9 September 2010	HL van Staden	Original document is created.
2.0.1	20 October 2010	D Liu	Addition of Amex & Diners details.
2.0.2	30 December 2010	D Liu	Replaced test credit card 4111...1111 with 4000...0010 and sample consistent key on page 17.
2.0.3	07 February 2011	HL van Staden	XML corrected in polling web services p22.
2.0.4	25 March 2011	D Liu	Removed errorcode 30006 on p 30. Added not case sensitive on p 14.
2.0.5	25 March 2011	HL van Staden	Addition of Device Profiling details.

## Table of Contents

Summary of Revisions.....	3
Table of Contents.....	4
Overview .....	6
Merchant Requirements.....	6
Merchant Admin Interface – Commerce Manager.....	7
Verified by Visa and MasterCard SecureCode .....	7
Credit Card Settlement .....	7
Credit and Debit Card Fraud Screening.....	8
Device Profiling for Fraud Screening.....	8
Sample HTML Profiling Tags.....	9
Credit Card vs Debit Card Processing.....	9
Credit Card Transaction Flow.....	10
Debit Card Transaction Flow .....	10
Message Fields .....	11
Transaction URL .....	13
Sending the Transaction Data .....	13
Response Format .....	14
Response Outcome .....	14
Consistent .....	16
How to generate the <i>Consistent2</i> Field.....	16
How to generate the <i>Consistent</i> Field – DO NOT USE THIS FIELD (RATHER USE Consistent2).....	17
Sample Consistent2 Values.....	17
Sample 1.....	17
Sample 2.....	17
Sample 3.....	17
3D Secure Handling Enrolled Responses .....	18
Redirect URL Response Format .....	18
3D Secure Message Request Format .....	19
3D Secure Message Response Format.....	19
Response Outcome .....	20
3D Secure Consistent .....	21
How to generate the 3D Secure <i>Consistent</i> Field .....	21
Fraud Screening Engine.....	22

Polling Transaction Status..... 22

Remote Settlement and Refund ..... 23

    Restrictions ..... 23

    Request Format..... 24

    Response Format ..... 25

    Response Outcome ..... 26

PCI-DSS (Payment Card Industry Data Security Standards) ..... 26

Open Source Modules..... 27

Testing..... 27

    Live Mode vs. Test Mode ..... 27

    Test Account Details ..... 27

    Credit Card ..... 27

    Debit Card ..... 28

Appendix A - Error Codes..... 29

Appendix B - ISO 3166 Country Codes ..... 36

Appendix C – Programming Samples ..... 42

    Classic ASP – ASPTear.DLL..... 42

    .NET Web Application –C# WebRequest method..... 42

    ColdFusion – CFHTTP ..... 45

    PHP – cURL..... 47

    JSP – HttpURLConnection..... 48

Contact Information..... 50

## Overview

This document provides technical implementation instruction that will guide the merchant in integrating to the Setcom Server-to-Server platform.

This document will cover the following.

1. Processing credit cards.
2. Processing debit cards.
3. Fraud screening.
4. Verified by Visa and MasterCard Secure Code integration.

The Setcom Server-to-Server platform is used by merchants who do website sales, content providers, call centre payments and subscription runs.

## Merchant Requirements

Merchants need to apply for an *E-Commerce Merchant Account* with one of the following banks.

- ABSA
- First National Bank
- Standard Bank of South Africa

Setcom will assist where possible with the application process. The application process usually takes between 2 and 6 weeks to complete.

Once the merchant account has been obtained, the merchant can process Visa and MasterCard transactions. In order to accept American Express and Diners cards, the merchant need to contact these card institutions directly to apply for additional merchant facilities. Contact details are:

- American Express Merchant Department: 011 359 0200
- Diners Merchant Department: 011 358 8400

Once the above institutions have issued you with merchant IDs, please submit them to both your bank and Setcom for loading.

Merchants will need a valid SSL certificate to securely collect the card details on their website. A valid SSL certificate with a minimum key strength of 128 bits needs to be obtained by the merchant. Certificates can be obtained from VeriSign, Thawte, GoDaddy or any reputable certificate authority.

Merchants will be responsible for all development, although Setcom will provide as much technical support as possible.

Communication via port 443 (SSL) on the merchant firewall needs to be allowed and configured. For security purposes the merchant can lock down outgoing SSL communication to the domain <https://secure.setcom.co.za/>. SSL version 2 is no longer supported by Setcom and we will only use SSL version 3 with high encryption ciphers.

## Merchant Admin Interface – Commerce Manager

A secure web interface called the **Setcom Commerce Manager** is available to merchants for reporting, monitoring and account configuration.

To access to the Setcom Commerce Manager please visit the below URL in your browser:

<https://manager.setcom.co.za/>

Always ensure you enter your login details on a secure URL starting with **https**.

Login details for the Setcom Commerce Manager will be issued to you once the Setcom Subscription Agreement has been completed and the merchant account has been loaded on the system. The initial login created will be the account administrator. The account administrator will be able to create additional user accounts and control access to what each new account can see and do.

## Verified by Visa and MasterCard SecureCode

Setcom uses the Verified by Visa and MasterCard SecureCode programs as an added layer of protection and cardholder authentication. References to **3D Secure** and the **3D Secure Programs** refer to the Verified by Visa and MasterCard SecureCode programs combined.

Both these programs apply to credit card processing only. Debit cards are not affected by these programs.

Debit card transactions are still however protected by the buyer PIN.

## Credit Card Settlement

The Setcom Server-to-Server platform can mark a credit card funded transaction for settlement in two ways.

1. Automatic Settlement ON: Any approved credit card transaction will automatically be marked for settlement. Merchants will see the money of credit card funded transactions in their bank account within 1 to 2 business days after settlement.
2. Automatic Settlement OFF: If a credit card transaction is approved, the funds will not be automatically marked for settlement. Funds for the transaction will be reserved on the buyer's credit card for 7 days. The cardholder will not be able to use the reserved funds on his credit card for 7 days after authorisation. It is up to the merchant to perform a manual settlement request to the Setcom server for partial or full settlement of the funds. Merchants will see the money of credit card funded transactions in their bank account within 1 to 2 business days after settlement.

Merchants can use the Setcom Commerce Manager to manage payments and orders. The Commerce Manager allows the merchant to settle, refund and re-authorize orders.

If the merchant requires remote settlement and refund of orders, please see section entitled **Remote Settlement and Refund** in this document.

Debit card funded transactions will always automatically be marked for settled. Debit card funded transactions will appear in your bank account 1 to 2 business days after settlement.

## Credit and Debit Card Fraud Screening

Setcom provides a rule based fraud screening engine that can be configured per outlet.

When your account is initially loaded Setcom will configure a default rule set for your type of business. Rules can be configured and fine tuned using the Fraud Management interface in the Setcom Commerce Manager.

The engine can perform the following tasks.

1. Black list: Black list fraudsters on any field in the payment message, e.g. card number, BIN range, common fraudulent billing address or shipping telephone number etc.
2. GeoBIN: scoring on the shipping and billing country related to where the credit or debit card was issued.
3. Velocity Checks: Buyer and credit and debit card velocity checks.
4. Limits: Enforce limits to minimize the impact of possible fraudsters trying to abuse your system. Enforce unique constraints on payment fields and stop duplication of orders based on the merchant reference and/or the payment amount per client for custom periods.
5. Alerting and Monitoring: Custom alerts let you pro actively stop fraudsters. Monitoring helps you fine tune scoring and blocking and allows you to “white list” good business.
6. Device Identification to uniquely identify the computer.

The Setcom Commerce Manager provides access to a user friendly interface where fraud rules can be configured and where monitoring can be done from.

## Device Profiling for Fraud Screening

Device profiling significantly enhances the fraud screening system by uniquely identifying the buyer's computer.

In order to deploy device profiling, the following steps needs to be followed:

1. Insertion of HTML profiling tags into web pages that a buyer will load prior to submitting the card details (such as a checkout payment page or login). These tags will allow Setcom to profile the buyer's computer.
2. Submit the buyer\_session\_id in the payment message to Setcom.

### Sample HTML Profiling Tags

```
<P STYLE="background:url(https://secure.setcom.co.za/fp/clear.png?org_id=tigbeibb&session_id=buyer_session_id&m=1)"></P>
<IMG ID="tmlMG" SRC="https://secure.setcom.co.za/fp/clear.png?org_id=tigbeibb&session_id=buyer_session_id&m=2" ALT="" >
<SCRIPT SRC="https://secure.setcom.co.za/fp/check.js?org_id=tigbeibb&session_id=buyer_session_id" TYPE="text/javascript">
</SCRIPT>

<OBJECT TYPE="application/x-shockwave-flash"
DATA="https://secure.setcom.co.za/fp/fp.swf?org_id=tigbeibb&session_id=buyer_session_id" WIDTH="1" HEIGHT="1" ID="obj_id">
<PARAM NAME="movie" VALUE="https://secure.setcom.co.za/fp/fp.swf?org_id=tigbeibb&session_id=buyer_session_id" />
<DIV></DIV>
</OBJECT>
```

**Replace the `buyer_session_id` in the above code with the buyer's session id created by your system.**

### Credit Card vs Debit Card Processing

Processing of credit and debit cards differ significantly. Credit cards do not require a PIN code for online processing, but the buyer might be required to complete 3D Secure authentication. Debit cards do not use the 3D Secure program, but the buyer is required to enter his card PIN (personal identification number issued by the bank) using a session to the cardholder's mobile handset.

Both credit and debit card funded transactions are screened for fraudulent patterns using the fraud screening engine.

	Credit Card	Debit Card
Uses Verified by Visa / MasterCard SecureCode to authenticate the cardholder	Yes	No
Uses card PIN to authenticate the cardholder	No	Yes
Payment process runs completely within the buyer's browser	Yes	No
A session with the buyer's mobile handset is used to collect the card PIN and CVV	No	Yes
Merchant collects CVV and passes to Setcom for processing	Yes	No
Protected by the screening engine	Yes	Yes
Device Identification	Yes	Yes

The cardholder's mobile number needs to be collected and passed to Setcom in the request message for debit card funded payments. No PIN or CVV must be collected for debit card funded payments. This will be done securely on the cardholder's mobile handset.

On credit card funded payments, card details needs to be collected securely on the merchant website including the card number and CVV. This needs to be transmitted to Setcom without being stored on the merchant database or other permanent or semi-permanent storage mediums.

## Credit Card Transaction Flow

1. The buyer visits the merchant website to purchases goods or services.
2. The merchant collects the credit card details from the buyer using a SSL secured page, including the card number, expiration date and CVV.
3. Optional for fraud screening. While the buyer enters the card details, profiling occurs on the payment page to uniquely identify the buyer's computer.
4. The merchant bundles the required message fields into a request message and sends the information to Setcom's Server-to-Server platform.
5. If the 3D Secure program is not enabled on the merchant account (for example MOTO merchants) or the buyer is not enrolled in the 3D Secure program (for example Diners and American Express cards), Setcom will perform an authorisation request to the bank and return the transaction result to the merchant.
6. If the 3D Secure program is enabled on the merchant account and buyer is enrolled in the 3D Secure program, Setcom will return a URL to the merchant where the buyer needs to be redirected to.
7. The generated URL will redirect the buyer to a URL hosted by the issuing bank (cardholder's bank). The buyer can now securely complete authentication on the issuing bank's website without compromising his 3D Secure password.
8. After successful cardholder authentication on the issuing bank's website, the buyer will be redirected back to the merchant website. The redirect request will contain a packet containing the PAREs (Payer Authentication Response). The PAREs needs to be submitted by the merchant to Setcom to complete the transaction.
9. The merchant initiates another HTTPS request to the Setcom server and includes the PAREs.
10. Setcom will perform an authorisation request to the bank, and include the correct ECI, CAVV and XID parameters for 3D Secure.
11. Setcom will return the transaction result to the merchant.

## Debit Card Transaction Flow

1. The buyer visits the merchant website to purchases goods or services.
2. The merchant collects the debit card details from the buyer using a SSL secured page, including the card number and expiration date (**do not collect the CVV or PIN**) and the cardholder's mobile number.
3. Optional for fraud screening. While the buyer enters the card details, profiling occurs on the payment page to uniquely identify the buyer's computer.
4. The merchant bundles the required message fields into a request message and sends the information to Setcom's Server-to-Server platform.
5. The merchant starts polling the transaction status from the Setcom server.
6. Setcom initiates a session with the cardholder's mobile handset to collect the card CVV and PIN.
7. The buyer enters his card CVV and PIN using his mobile handset.
8. Setcom bundles this information with the already collected information and send an authorisation request to the bank.
9. Setcom updates the transaction status with the bank response.
10. The merchant picks up the status change for the transaction from the Setcom server in the status polling process (step 4 above).

11. The merchant displays the appropriate transaction response to the buyer on the merchant website.

## Message Fields

FIELD NAME	CREDIT / DEBIT CARD / BOTH	REQUIRED	MAX LENGTH	DESCRIPTION
<b>CO_ID</b>	Both	Yes	50	Value issued to merchant by Setcom used to identify company on system.
<b>OUTLET</b>	Both	Yes	50	Value issued to merchant by Setcom used to identify outlet on system.
<b>Reference</b>	Both	Yes	250	Value generated by the merchant system to keep track of this transaction. This value will be passed back to the merchant in the transaction response. This value will appear on all merchant reports and will be used by the merchant for reconciliation purposes. Setcom strongly urges merchants to use a unique value per transaction for this field.
<b>CC_Amount</b>	Both	Yes	Decimal (18,2)	Value of the transaction in decimal format, e.g. 19500.70
<b>CCName</b>	Credit Card	Yes	50	Cardholder name as embossed on the front of the credit card.
<b>CCNumber</b>	Both	Yes	21	Credit card number as embossed on the front of the credit card.
<b>ExYear</b>	Credit Card	Yes	4	Credit card expiry year as embossed on the front of the credit card, format CCYY, e.g. 2015.
<b>ExMonth</b>	Credit Card	Yes	2	Credit card expiry month as embossed on the front of the credit card, format MM, e.g. 01.
<b>CCCVV</b>	Credit Card	Yes	4	Credit card CVV. For Visa and MasterCard this is the last 3 digits on the back of the credit card. For American Express this is the last 4 digits on the front of the credit card.
<b>PayPeriod</b>	Credit Card	No	2	Budget period of transaction, only available on South African credit cards for transaction amounts greater than R 300.00. Valid periods include 0 (no budget), 6, 12, 18, 24, 36 and 48 months.
<b>EmailAddress</b>	Credit Card	No	250	Email address of cardholder. Used for fraud screening purposes. We do not use this address to communicate with your buyers neither do we sell or share this information.

<b>MobileNumber</b>	Debit Card	Yes	12	This is the mobile number of the debit cardholder. The RevoPIN will be sent to this mobile number for the transaction.
<b>CCType</b>	Credit Card	No	16	The card brand of the credit card, valid value includes "Visa", "MasterCard", "Diners" and "American Express".
<b>AccType</b>	Debit Card	Yes	6	Indicates the type of account linked to the debit card, valid values include "Savings" and "Cheque".
<b>Consistent</b>	Both	No	512	Setcom provides a routine to enable the merchant to encrypt the price and reference of the transaction and pass this encrypted value to our servers. If the encrypted price and reference does not match then information has been altered and the transaction is not processed. See the section entitled <b>Consistent</b> for instructions on how to generate this field.
<b>buyer_id</b>	Both	No	100	Unique ID created for this buyer on the merchant system.
<b>buyer_session_id</b>	Both	No	512	Unique session ID assigned to the buyer. This field is required for device profiling.
<b>ship_title</b>	Both	No	10	Title of the order recipient.
<b>ship_first_name</b>	Both	No	500	First name of the order recipient.
<b>ship_last_name</b>	Both	No	500	Last name of the order recipient.
<b>ship_street1</b>	Both	No	500	Street address 1 of the order recipient.
<b>ship_street2</b>	Both	No	500	Street address 1 of the order recipient.
<b>ship_city</b>	Both	No	500	City or town of the order recipient.
<b>ship_state</b>	Both	No	500	State or province of the order recipient.
<b>ship_zip</b>	Both	No	500	Zip or postal code of the order recipient.
<b>ship_country</b>	Both	No	2	ISO 3166 Country code of the order recipient, see Appendix A: ISO 3166 Country Codes.
<b>ship_phone</b>	Both	No	500	Telephone number of the order recipient.
<b>bill_title</b>	Both	No	10	Title of the cardholder.
<b>bill_first_name</b>	Both	No	500	First name of the cardholder.
<b>bill_last_name</b>	Both	No	500	Last name of the cardholder.
<b>bill_street1</b>	Both	No	500	Street address 1 of the cardholder.
<b>bill_street2</b>	Both	No	500	Street address 2 of the cardholder.
<b>bill_city</b>	Both	No	500	City or town of the cardholder.
<b>bill_state</b>	Both	No	500	State or province of the cardholder.
<b>bill_zip</b>	Both	No	500	Zip or postal code of the cardholder.

<b>bill_country</b>	Both	No	2	ISO 3166 Country code of the order billing address, see Appendix A: ISO 3166 Country Codes.
<b>bill_phone</b>	Both	No	500	Telephone number of the cardholder.
<b>ip_address</b>	Both	No	15	The IP address of the buyer in xxx.xxx.xxx.xxx format.

## Transaction URL

Transaction data should be sent to the following URL only.

<https://secure.setcom.co.za/server.cfm>

## Sending the Transaction Data

Transaction messages need to be submitted to the Setcom Server-to-Server API via HTTPS calls. This can be facilitated in various forms depending on the merchant programming language used.

The below table summarized the technologies used by various programming languages to perform HTTPS post operations.

Programming Language	Technologies to Use	Comment
Classic ASP	ASPTear.DLL	Please contact Setcom customer services for a copy of ASPTear.DLL.
.NET Web Application	C# HTTPWebRequest method	Please see Appendix C – Programming Samples for more information on this technology.
ColdFusion	CFHTTP method	Please see Appendix C – Programming Samples for more information on this technology.
PHP	PHP/CURL	Please see Appendix C – Programming Samples for more information on this technology.
JSP	HttpConnection	Please see Appendix C – Programming Samples for more information on this technology.

If your programming language is not listed in the above table, please contact customer services for further assistance.

## Response Format

The Setcom Server-to-Server API response will always be in the form of a 7 element comma separated list. Each element in the list contains the response variables as laid out in the below table.

Element	Field Name	Description
1	Response outcome	String value representing the transaction <b>response outcome</b> . See the below section called "Response Outcome" for a more detailed explanation of what this field means.
2	Response Indicator	The use of this field and the value populated in this field is determined by the value of the <b>response outcome</b> (element one in the response message). For example; if the <b>response outcome</b> is returned as APPROVED, then this field will contain the bank authorization number. See the below section called "Response Outcome" for a detailed explanation of this field and possible values associated with this field.
3	Date	Transaction date as on the Setcom server in format dd/mm/yyyy.
4	Time	Transaction time as on the Setcom server in format HH:mm:ss tt.
5	Setcom Order ID	Unique Setcom ID created for this order. In some cases this field will return a 0 (zero) if no order could be created on the Setcom system, e.g. when the CO_ID or OUTLET values are invalid.
6	Merchant Reference	The merchant reference for this transaction will be passed back to the merchant in this field.
7	Transaction Amount	Amount of the transaction as recorded on the Setcom server. This field excludes any currency symbols, e.g. 19525.30.

## Response Outcome

The table below describes the various response outcomes returned by Setcom. Always ensure when checking the first response element that your comparison is **not case sensitive**. I.e.: "Approved" is the same as "APPROVED".

1 <sup>st</sup> Response Element	2 <sup>nd</sup> Element Will Contain...	Comment
APPROVED	Authorisation number	Bank authorisation number as returned by the bank on the authorisation request.
DECLINED	Decline code	Decline code from bank; see Appendix B – Error and Decline Codes for an explanation of the decline code.
ERROR	Error code	Error code from Setcom or processor; see Appendix B – Error and Decline Codes for an explanation of the decline code.

STOP	Fraud screening score	Fraud screening score of the transaction as returned from the Fraud Screening Engine.
REVIEW	Fraud screening score	Fraud screening score of the transaction as returned from the Fraud Screening Engine.
ENROLLED	ACS (access control system) URL	URL of the Access Control System where the buyer needs to be redirected to for Secure 3D (Verified by Visa and MasterCard SecureCode) authentication.
UNAVAILABLE	The text "UNAVAILABLE".	Secure 3D Authentication was unavailable on this credit card. Please try again and contact the merchant if this error persists.
ATTEMPTED	The text "ATTEMPTED".	Secure 3D Authentication was attempted but failed on this credit card. Please try again and contact the merchant if this error persists.
DUPLICATE	Setcom Order ID of duplication	Setcom Order ID of the previous order that matches the same amount and card number as this transaction.
POLL	The text "POLL".	This indicates that the transaction can not occur in real-time. The merchant will have to poll the transaction status from the Setcom Server-to-Server API. See the section entitled "Polling Transaction Status".

A few sample response strings are included below for explanations purposes. The first sample is that of an approved transaction. Note that element one contains the word **APPROVED** and the second element contains the bank authorisation number **123456**. Please ensure that this field is not checked with case sensitivity. I.e.: "Approved" is the same as "APPROVED".

*APPROVED,123456,09/09/2010,14:16:15 PM,10069707,MERCH\_REF\_0012,950.00*

The sample string below depicts a typical error, that of an invalid card number. Note that element one of the response string contains the word **ERROR** and the second element thus contains the error code, in this case **32057**, meaning Invalid Card Number.

*ERROR,32057,09/09/2010,14:17:15 PM,10069708,MERCH\_REF\_0013,850.00*

This sample message is that of a declined transaction. Note that element one contains the word **DECLINED** and the second element contains the decline code **32011**, meaning Transaction Declined.

*DECLINED,32011,09/09/2010,14:18:15 PM,10069709,MERCH\_REF\_0014,750.00*

This sample message shows an order that has been stopped by the fraud screening engine. This order is above the merchant maximum order limit.

*STOP,10145,09/09/2010,14:18:17 PM,10069710,MERCH\_REF\_0015,19000.00*

This sample message shows an orders where 3D Secure authentication is required. The first response element contains the text **ENROLLED**. The second response element contains the redirect URL where the buyer must be redirected to.

*ENROLLED,https%3A%2F%2Fsecure%2Esetcom%2Ecom%2F3dauth%2Ecfm%3FREF%3DX4364%26p%3D4985956%26c%3DERERDFER%2D848J%2DYE64%2DE4R5%2DJR7475HH,09/09/2010,14:19:11 PM,10069711,MERCH\_REF\_0016,120.00*

## Consistent

An additional consistent field can be included in the transaction request to ensure the request originated from the merchant and no fields were changed.

Before implementing the consistent field, Setcom will generate a new secret key for the merchant. This secret key must not be shared with anyone and must only be known to the merchant and Setcom.

The consistent field is generated by concatenating selected message request fields. A secret **consistent key**, known only to the merchant and Setcom, is then appended to newly created string. The combined string is then hashed and included in the transaction request message to Setcom.

**Please note that the consistent key is never included in the transaction message in the clear.**

After Setcom receives the transaction message request, Setcom will in turn build its own version of the consistent field, using the selected message request fields and the secret key from the Setcom database.

If the merchant submitted consistent value matches the Setcom generated consistent value, Setcom will process the transaction request. If the two consistent values do not match, Setcom will reject the transaction request.

***Please ensure that your system uses unique merchant Reference values.***

New merchants and new implementations are required to use the **Consistent2** transaction request message field, which relies on the SHA512 hashing algorithm. The **Consistent** transaction request message field is being discontinued as this still uses a MD5 hashing algorithm.

## How to generate the Consistent2 Field

1. The following transaction request message fields need to be concatenated first.
  - a. CO\_ID
  - b. OUTLET
  - c. Reference
  - d. CC\_Amount

- e. CCNumber
2. Once a string has been generated using the above fields, append the secret consistent key to the string.
3. Apply a SHA512 hashing algorithm to the newly generated string. Remember to use UTF-8 encoding.
4. The newly generated hash will always be an all uppercase string.

### How to generate the *Consistent* Field – DO NOT USE THIS FIELD (RATHER USE Consistent2)

1. The following transaction request message fields need to be concatenated first.
  - a. Reference
  - b. CC\_Amount
  - c. OUTLET
2. Once a string has been generated using the above fields, append the secret consistent key to the string.
3. Apply a MD5 hashing algorithm to the newly generated string. Remember to use UTF-8 encoding.
4. The newly generated hash will always be an all uppercase string.

### Sample Consistent2 Values

#### Sample 1.

**CO\_ID:** testaccount  
**OUTLET:** testaccount  
**Reference:** PRO\_001  
**CC\_Amount:** 10.00  
**CCNumber:** 5454545454545454  
**Consistent Key:**  
 ntVAb33o2mTf1oG6qa5H2GyhfiF3kiz3ywvovxJMK0VwWWDe0srWbauGWWOsW9s  
**CONSISTENT2:**  
 EA699704B641420069E38FD27CE59F08FC5F0531CFFBE4D556AC1D8904E6F59392A59C2FAA344130  
 6B48BCC501D592B48A4E8B8DD845C2609B1BA55254A8C21A

#### Sample 2.

**CO\_ID:** testaccount  
**OUTLET:** testaccount  
**Reference:** F1197C71FEFB61462E0  
**CC\_Amount:** 199.95  
**CCNumber:** 5454545454545454  
**Consistent Key:**  
 9bcdJgxrF7oBThRSK0hN48mrJqwuAu4LgblyEcDcLxJUQOHPlrEc1pF7AbVzSLw  
**CONSISTENT2:**  
 CB8789914DC0A20684A840E7C0499A240F5EBED50C2B38417F26E5FA1BE36AB3CA452914A81E90F  
 2C08A9FD9EBB4C57D95E267E194615603CC76C4ECB01E8516

#### Sample 3.

**CO\_ID:** TestAccount \* *Note the capitalization*  
**OUTLET:** TestAccount \* *Note the capitalization*

**Reference:** E4-2232-EEE-934  
**CC\_Amount:** 80 \* *Setcom will use the field in the same format as sent by the merchant*  
**CCNumber:** 343434343434343  
**Consistent Key:**  
 9bcdJgxrF7oBThRSK0hN48mrJqwuAu4LgblyEcDcLxJUQOHPIrEc1pF7AbVzSLw  
**CONSISTENT2:**  
 39EA59D19E27CC68A77BA439F7466DC354984B380E7103DB937F245923902901A7009E7355DD6C3  
 51FF808B69984D9E7DB031764990EAC1EBE38D579B452EDF8

### 3D Secure Handling Enrolled Responses

When a credit card is enrolled in the 3D Secure program, Setcom will return a response outcome of **ENROLLED** in the first response element to the merchant. The second response element will contain a URL where the buyer must be redirected to. This URL will redirect the buyer to the ACS (access control system), which is served off the credit card issuer's website.

A sample buyer redirect URL is included below.

[https://secure.setcom.co.za/3dauth.cfm?s=ABCDE-12345-FGHIJ-67890&c=ABCDE12345&p=12345&CO\\_ID=testaccount&OUTLET=testaccount&Reference=PRO-001&CC\\_Amount=10.00](https://secure.setcom.co.za/3dauth.cfm?s=ABCDE-12345-FGHIJ-67890&c=ABCDE12345&p=12345&CO_ID=testaccount&OUTLET=testaccount&Reference=PRO-001&CC_Amount=10.00)

Once redirected to the ACS, the buyer will enter his credit card 3D Secure password on the ACS window. If cardholder authentication fails on the ACS, the buyer will be redirected back to the merchant, and Setcom will include the error details in the redirect request.

### Redirect URL Response Format

If cardholder authentication is successful, the buyer will be redirected back to the merchant website. The following variables will be passed back to the merchant after the buyer completes ACS authentication.

Field Name	Description
<b>error_code</b>	Response error code. 0 (zero) indicates a successful response.
<b>error_description</b>	Text description of the error code.
<b>pares</b>	The Payer Authentication Response.
<b>order_id</b>	Unique Order ID generated by Setcom.
<b>reference</b>	Value generated by the merchant system to keep track of this transaction. This value will be passed back to the merchant in the transaction response. This value will appear on all merchant reports and will be used by the merchant for reconciliation purposes. Setcom strongly urges merchants to use a unique value per transaction for this field.
<b>cc_amount</b>	Value of the transaction in decimal format excluding any currency symbol, e.g. 1999.99.

### 3D Secure Message Request Format

If cardholder authentication is completed and successful, the merchant must submit a request to the Setcom server to complete the transaction authorisation. This second request is made to the below URL.

<https://secure.setcom.co.za/3dserver.cfm>

The message fields that are required are included below.

Field Name	Required	Description
co_id	Yes	Value issued to merchant by Setcom used to identify company on system.
outlet	Yes	Value issued to merchant by Setcom used to identify company on system.
order_id	Yes	Unique Order ID generated by Setcom and returned to the merchant in the initial transaction response and on the buyer redirect back after ACS authentication.
reference	Yes	Value generated by the merchant system to keep track of this transaction. This value will be passed back to the merchant in the transaction response. This value will appear on all merchant reports and will be used by the merchant for reconciliation purposes. Setcom strongly urges merchants to use a unique value per transaction for this field.
cc_amount	Yes	Value of the transaction in decimal format excluding any currency symbol, e.g. 1999.99.
pares	Yes	The Payer Authentication Response (PAREs) passed back to the merchant after ACS authentication.
consistent	Yes	Setcom provides a routine to enable the merchant to encrypt pieces of the transaction and pass this encrypted value to our servers. If the encrypted piece of data does not match the equivalent string generated on the Setcom server, information has been altered and the transaction is not processed. See the section entitled <b>3D Secure Consistent</b> for instructions on how to generate this field.

### 3D Secure Message Response Format

Once the above variables are received and validated by Setcom, Setcom will perform an authorisation request to the bank, including the correct 3D Secure ECI, CAVV and XID parameters. Setcom will provide the transaction response to the merchant. The transaction response will always be in the form of a 7 element comma separated list. Each element in the list contains the response variables as laid out in the below table.

Element	Field Name	Description
1	Response outcome	String value representing the transaction <b>response outcome</b> . See the below section called "Response Outcome" for a more detailed explanation of what this field means.
2	Response Indicator	The use of this field and the value populated in this field is determined by the value of the <b>response outcome</b> (element one in the response message). For example; if the <b>response outcome</b> is returned as APPROVED, then this field will

		contain the bank authorisation number. See the below section called "Response Outcome" for a detailed explanation of this field and possible values associated with this field.
<b>3</b>	Date	Transaction date as on the Setcom server in format dd/mm/yyyy.
<b>4</b>	Time	Transaction time as on the Setcom server in format HH:mm:ss tt.
<b>5</b>	Setcom Order ID	Unique Setcom ID created for this order. In some cases this field will return a 0 (zero) if no order could be created on the Setcom system, e.g. when the CO_ID or OUTLET values are invalid.
<b>6</b>	Merchant Reference	The merchant reference for this transaction will be passed back to the merchant in this field.
<b>7</b>	Transaction Amount	Amount of the transaction as recorded on the Setcom server. This field excludes any currency symbols, e.g. 19525.30.

### Response Outcome

1 <sup>st</sup> Response Element	2 <sup>nd</sup> Element Will Contain...	Comment
APPROVED	Authorisation number	Bank authorisation number as returned by the bank on the authorisation request. Please ensure that this field is not checked with case sensitivity. I.e.: "Approved" is the same as "APPROVED".
DECLINED	Decline code	Decline code from bank; see Appendix B – Error and Decline Codes for an explanation of the decline code.
ERROR	Error code	Error code from Setcom or processor; see Appendix B – Error and Decline Codes for an explanation of the decline code.

A few sample response strings are included below for explanations purposes. The first sample is that of an approved transaction. Note that element one contains the word **APPROVED** and the second element contains the bank authorisation number **123456**.

*APPROVED,123456,09/09/2010,14:16:15 PM,10069707,MERCH\_REF\_0012,950.00*

The sample string below depicts a typical error, that of an invalid card number. Note that element one of the response string contains the word **ERROR** and the second element thus contains the error code, in this case **32057**, meaning Invalid Card Number.

*ERROR,32057,09/09/2010,14:17:15 PM,10069708,MERCH\_REF\_0013,850.00*

This sample message is that of a declined transaction. Note that element one contains the word **DECLINED** and the second element contains the decline code **32011**, meaning Transaction Declined.

*DECLINED,32011,09/09/2010,14:18:15 PM,10069709,MERCH\_REF\_0014,750.00*

### 3D Secure Consistent

An additional consistent field can be included in the transaction request to ensure the request originated from the merchant and no fields were changed.

Before implementing the consistent field, Setcom will generate a new secret key for the merchant. This secret key must not be shared with anyone and must only be known to the merchant and Setcom.

The consistent field is generated by concatenating selected message request fields. A secret **consistent key**, known only to the merchant and Setcom, is then appended to newly created string. The combined string is then hashed and included in the transaction request message to Setcom.

**Please note that the consistent key is never included in the transaction message in the clear.**

After Setcom receives the transaction message request, Setcom will in turn build its own version of the consistent field, using the selected message request fields and the secret key from the Setcom database.

If the merchant submitted consistent value matches the Setcom generated consistent value, Setcom will process the transaction request. If the two consistent values do not match, Setcom will reject the transaction request.

***Please ensure that your system uses unique merchant Reference values.***

New merchants and new implementations are required to use the **Consistent2** transaction request message field, which relies on the SHA512 hashing algorithm. The **Consistent** transaction request message field is being discontinued as this still uses a MD5 hashing algorithm.

### How to generate the 3D Secure Consistent Field

1. The following transaction request message fields need to be concatenated first.
  - a. Secret consistent key
  - b. CO\_ID
  - c. OUTLET
  - d. Reference
  - e. Secret consistent key
  - f. Amount
  - g. Date in format CCYYMMDDYYDD
2. Once a string has been generated using the above fields apply a SHA512 hashing algorithm to the newly generated string. Remember to use UTF-8 encoding.
3. The newly generated hash will always be an all uppercase string.

## Fraud Screening Engine

Setcom utilises a rules based fraud screening engine to minimize the potential risk involved with trading online. The fraud engine is fully customizable per merchant. Full reporting on the performance of your configured fraud rules is provided as well.

Fraud screening is done before any other process, e.g. Secure 3D or bank authorisation. This means any potential risk is minimized by stopping orders before they are processed.

The fraud engine can also be configured to alert on suspicious behaviour. Merchants will receive real-time notification via email or SMS and can pro-actively react to potential threats.

Once your Setcom account has been loaded, customer services will contact you with instructions on how to configure the fraud screening engine. Configuration settings can be viewed and changed in the Setcom Commerce Manager by the merchant in real-time.

## Polling Transaction Status

Poll status cause:

1. Timeout or break in communication between merchant and Setcom.
2. Non real-time transaction, where buyer has to complete an external process before the transaction can be approved/decline.

Merchants can poll the transaction status using the *card\_order\_query* method in the *Order Query Web Service*. The web service WSDL file is located at the below URL:

<https://secure.setcom.co.za/server/api.cfc?wsdl>

(If your programming language doesn't support web service implementations; please contact customer service to discuss different implementation options).

Ensure that you always connect to the secure URL (https). This will ensure the communication between the merchant and the Setcom server is encrypted.

When calling the *card\_order\_query* method the merchant needs to supply a XML request string to the method. The XML request string will contain the merchant's login details as well as a list of order reference numbers and amounts the merchant wants to query on the Setcom system.

A sample XML request string is included below.

```
<?xml version="1.0" encoding="UTF-8"?>
<card_order_query_request>
  <merchant>
    <co_id>testaccount</co_id>
    <outlet>testaccount</outlet>
    <uname>testaccount</uname>
    <pwd>testaccount</pwd>
```

```

</merchant>
<orders>
  <transaction>
    <reference>REF-001-001</reference>
    <amount>10.00</amount>
  </transaction>
  <transaction>
    <reference>REF_001-002</reference>
    <amount>20.00</amount>
  </transaction>
  <transaction>
    <reference>REF_001-003</reference>
    <amount>30.00</amount>
  </transaction>
</orders>
</card_order_query_request>

```

XML Element	Required	Description
card_order_query_request	Yes	Root element of the XML request string.
merchant	Yes	Element containing the merchant login and account details.
co_id	Yes	Value issued to merchant by Setcom used to identify company on system.
outlet	Yes	Value issued to merchant by Setcom used to identify outlet on system.
uname	Yes	Outlet username of user who has access to merchant reporting.
pword	Yes	Outlet password of user who has access to merchant reporting.
orders	Yes	Element containing a record per order that is being queried.
transaction	Yes	Element containing the order details of the order being queried.
reference	Yes	The merchant reference number created and submitted by the merchant in the original Setcom remote API request.
amount	Yes	The transaction amount submitted the merchant in the original Setcom remote API request.

## Remote Settlement and Refund

Setcom provides a remote interface that merchants can use to remotely process settlement and refund messages on already authorised orders.

### Restrictions

1. A merchant can perform partial settlements, as long as the sum of all the partial settlements does not exceed the original authorisation amount.
2. A merchant can perform partial refunds, as long as the sum of all the partial refunds does not exceed the original authorisation amount.

3. An approved authorisation request will reserve the funds on the credit card for 7 days only.  
**Any settlement requests need to be done within 7 days of the original authorisation.**
4. Refunds can only be processed for 6 months after the original authorisation date.

### Request Format

To perform a remote settlement or refund request the merchant has to perform a HTTPS post operation to the below URL.

<https://manager.setcom.co.za/captures2s.cfm>

The following fields are required to perform a remote settlement.

Field Name	Required	Description
CO_ID	Yes	Value issued to merchant by Setcom used to identify company on system.
OUTLET	Yes	Value issued to merchant by Setcom used to identify outlet on system.
OrderID	Yes	Unique Order ID generated by Setcom and returned to the merchant in the initial transaction response.
TnxType	Yes	Text value indicating transaction request action: <ol style="list-style-type: none"> <li>1. SHIP</li> <li>2. REFUND</li> <li>3. CANCEL</li> </ol> Only orders that have not been settled can be cancelled. This just marks the transaction as cancelled (unable to settle later) in the system.
Amount	Yes	The transaction request amount. If this is a partial settlement or refund, the amount needs to be smaller than the original authorisation amount. If the full amount needs to be settled, populate the full authorisation amount in decimal format excluding any currency symbol, e.g. 19999.99.
Username	Yes	Merchant username as issued to the merchant on signup. The merchant can create additional user account in the Commerce Manager.
Password	Yes	The password of the above username.

## Response Format

The Setcom response will always be in the form of a 9 element comma separated list. Each element in the list contains the response variables as laid out in the below table.

Element	Field Name	Description
1	Outcome	String value representing the transaction <i>response outcome</i> . See the below section called "Response Outcome" for a more detailed explanation of what this field means.
2	Error Code	If the transaction request is not approved, this field will contain the error code. For approved transactions this field will simply contain the text <b>APPROVED</b> . Please ensure that this field is not checked with case sensitivity. I.e.: "Approved" is the same as "APPROVED".
3	Authorisation Number	If this transaction request is approved, this field will contain the bank authorisation number. For transactions not approved this field will contain the text "0" (zero).
4	Date	Transaction date as on the Setcom server in format dd-mmm-yy.
5	Time	Transaction time as on the Setcom server in format HH:mm tt.
6	Setcom Order ID	Unique Setcom ID created for this order. In some cases this field will return a 0 (zero) if no order could be created on the Setcom system, e.g. when the CO_ID or OUTLET values are invalid.
7	Transaction Key	Transaction key as generated by the bank. A uniq transaction key is generated per auth/settlement pair and per refund.
8	Transaction Type	This field will contain the below text depending on the transaction type submitted: <ol style="list-style-type: none"> <li>1. SHIP</li> </ol>

		2. REFUND 3. CANCEL
9	Amount	The transaction request amount in decimal format excluding any currency symbol, e.g. 19999.99.

## Response Outcome

1 <sup>st</sup> Response Element	2 <sup>nd</sup> Element Will Contain...	Comment
APPROVED	Authorisation number	Bank authorisation number as returned by the bank on the authorisation request. Please ensure that this field is not checked with case sensitivity. I.e.: "Approved" is the same as "APPROVED".
DECLINED	Decline code	Decline code from bank; see Appendix B – Error and Decline Codes for an explanation of the decline code.
ERROR	Error code	Error code from Setcom or processor; see Appendix B – Error and Decline Codes for an explanation of the decline code.

A few sample response strings are included below for explanations purposes. The first sample is that of an approved settlement message. Note that element one contains the word **APPROVED** and the third element contains the bank authorisation number **123456**.

*APPROVED, APPROVED,123456,2-Sep-2010,14:16 PM,10069707,STK123123123,SHIP,12.95*

The sample string below depicts a typical error, that of an invalid OrderID parameter. Note that element one of the response string contains the word **ERROR** and the second element thus contains the error code, in this case **32057**, meaning Invalid Card Number.

*ERROR,614,0,3-Feb-2010,14:17 PM,10069708,0,SHIP ,850.00*

## PCI-DSS (Payment Card Industry Data Security Standards)

Merchants are not allowed at any time to store the credit card or debit card number, card expiration dates, CVV or CVV2 values. Storing any of these values brings your implementation and integration into scope for a full PCI-DSS review and audit.

Best practises dictate that card data is collected and transmitted to Setcom without ever being stored to a database, file or other permanent or semi-permanent storage medium.

If the card data needs to be stored for business purposes; please contact us on the details at the end of this document to discuss your requirements. We will assist the merchant to start the PCI-DSS compliance process.

For more information on PCI-DSS, please visit the URL below:

<https://www.pcisecuritystandards.org/>

## Open Source Modules

Setcom currently provides modules for the below open-source shopping cart systems.

1. osCommerce

For more information regarding these modules and to download modules, please visit our **Getting Started** section on [www.setcom.co.za](http://www.setcom.co.za)

If a module for your shopping cart is not listed here, please send through a request to customer services (contact details are included at the bottom of this document or on [www.setcom.co.za](http://www.setcom.co.za)).

## Testing

### Live Mode vs. Test Mode

Setcom allows for an account to be placed into test mode which has the implication that **every** transaction will be Approved, regardless of the information passed. If in test mode, the authorization number will be "123456" and the bank transaction key will be "LoopBack". When in this mode, no real transactions will ever be processed.

It is **extremely important** that you make certain that your account is in **live mode** before you proceed going live. If this is not done and your account is in test mode when you go live, it will result in clients being able to process live transactions without paying you.

Please note that to both enter and to leave test mode it is required to have the contract holder make the request to [support@setcom.com](mailto:support@setcom.com).

### Test Account Details

To test please use the below details or contact [support@setcom.com](mailto:support@setcom.com) for a test account.

- CO\_ID: testaccount
- OUTLET: testaccount
- Username: testaccount
- Password: testaccount

**This is a public testing account so please refrain from using real credit or debit card details.** For testing please use any of the below card numbers. These are test card numbers only, intended to be used by developers to test their implementation.

## Credit Card

Visa
------

<b>Test Buyer VS1</b>	4000 0000 0000 0010	11-2020	111
<b>Test Buyer VS2</b>	4444 3333 2222 1111	11-2020	111
<b>Test Buyer VS3</b>	4000 0000 0000 0002	11-2020	111
<b>MasterCard</b>			
<b>Test Buyer MC1</b>	5454 5454 5454 5454	12-2020	222
<b>Test Buyer MC2</b>	5566 5566 5566 5566	12-2020	222
<b>Test Buyer MC3</b>	5555 5555 5555 4444	12-2020	222
<b>Diners</b>			
<b>Test Buyer DC1</b>	3600 0000 0000 08	11-2020	Na
<b>Test Buyer DC2</b>	3020 4169 3226 43	11-2020	Na
<b>Test Buyer DC3</b>	3056 9309 0259 04	11-2020	Na
<b>American Express</b>			
<b>Test Buyer AX1</b>	3434 3434 3434 343	12-2020	1111
<b>Test Buyer AX2</b>	3411 1111 1111 111	12-2020	1111
<b>Test Buyer AX3</b>	3400 0000 0000 009	12-2020	1111

## Debit Card

<b>Visa</b>			
<b>Test Buyer DB VS1</b>	4917 3000 0000 0008	11-2020	444
<b>Test Buyer DB VS2</b>	4917 3008 0000 0000	11-2020	444
<b>MasterCard</b>			
<b>Test Buyer DB MC1</b>	5641 8200 0000 005	12-2020	555

Transactions done in test mode will always return an authorisation number of **123456** and a transaction key of **LoopBack**.

## Appendix A - Error Codes

Please contact customer services if you require this list in a machine readable format, e.g. CSV (comma-separated-values).

Error Code	Description
10000	Processing error
10101	One or more compulsory field(s) missing
10102	The merchant / outlet could not be found on the system
10103	Merchant requires consistent checking to be done
10104	Security failure occurred while performing consistent checking
10105	Payment method not accepted by outlet
10106	Merchant inactive
10107	File missing on server
10108	Missing variable
10109	Unknown error occurred
10110	Card blacklisted
10201	Transaction amount invalid
10202	Expiry month invalid
10203	Expiry year invalid
10204	PayPeriod invalid
10205	Transaction amount too small
10206	Email address invalid.
10207	Original transaction date of out of range
10301	Unable to retrieve order information
10302	Base table not found
10303	Column not found
10304	Syntax error or access violation
10305	Error in assignment
10306	Serialization error occurred
10307	General exception error occurred
10308	Communication link failure
10309	Datasource not found or no default driver specified
10310	Numeric value out of range
10311	Authorisation failure
10312	Call to the bank failed.
10313	Fully-qualified address and the socket has not been marked to allow address reuse.
10401	Invalid Gateway call
10402	Verification unavailable
10403	Error occurred while attempting verification.
10404	Signature validation error occurred
10405	Transaction not authenticated.
10406	The transaction requires the verification data to be included in the message.
10407	Unable to verify cardholder.
16001	Invalid transaction type
16002	Invalid storename
16003	Card number or CVV blank/incorrect

16004	Transaction amount zero
16005	Card number in invalid format
16006	Card number in invalid format
16008	Invalid or missing config
16009	Invalid property assignment
16010	Unsupported transaction
16011	Terminal incorrectly loaded
16012	MerchantID incorrect
	Mandatory properties have not been set. Certain properties are mandatory for messages sent to the server. This error is raised when mandatory properties have not been set
16013	
16014	BIN table not found
16016	Refer to issuer
16017	Host down
16018	Invalid account
17001	Refer to card issuer
17002	Refer to card issuer
17003	Invalid merchant
17004	Pick-up card
17005	Do not honor
17006	Error
17007	Pick-up card - special condition
17008	Honor with identification
17009	Request in progress
17010	Approved - partial
17011	Approved - VIP
17012	Invalid transaction
17013	Invalid amount
17015	No such issuer
17016	Approved - update track 3
17017	Customer cancellation
17018	Customer dispute
17019	Re-enter transaction
17020	Invalid response
17021	No action taken
17022	Suspected malfunction
17023	Unacceptable transaction fee
17024	File update not supported
17025	Unable to locate record
17026	Duplicate record
17027	File update field edit error
17028	File update file locked
17029	File update failed
17030	Format error
17031	Bank not supported
17032	Completed partially

17033	Expired card - pick-up
17034	Suspected fraud - pick-up
17035	Contact acquirer - pick-up
17036	Restricted card - pick-up
17037	Call acquirer security - pick-up
17038	PIN tries exceeded - pick-up
17039	No credit account
17040	Function not supported
17041	Lost card - pick-up
17042	No universal account
17043	Stolen card - pick-up
17044	No investment account
17051	insufficient funds
17052	No check account
17053	No savings account
17054	Expired card
17055	Incorrect PIN
17056	No card record
17057	Transaction not permitted to cardholder
17058	Transaction not permitted on terminal
17059	Suspected fraud
17060	Contact acquirer
17061	Exceeds withdrawal limit
17062	Restricted card
17063	Security violation
17064	Original amount incorrect
17065	Exceeds withdrawal frequency
17066	Call acquirer security
17067	Hard capture
17068	Response received too late
17075	PIN tries exceeded
17077	Intervene - bank approval required
17078	Intervene - bank approval required for partial amount
17090	Cut-off in progress
17091	Issuer or switch inoperative
17092	Routing error
17093	Violation of law
17094	Duplicate transaction
17095	Reconcile error
17096	System malfunction
17097	Reserved for future Postilion use
17098	Exceeds cash limit
18057	Merchant ID is invalid or missing. Message rejected.
18057	Unable to locate Merchant Configuration Information Within System
30001	Unable to connect to Gateway
30006	Connection to the bank timed out

30033	Invalid Merchant
32001	Invalid card number or cvv
32002	Phone the bank
32003	Card blocked
32004	Invalid card or CVV number
32005	Card expired
32008	Card too new
32011	The transaction was declined by the bank.
32011	Transaction declined
32011	The transaction was declined by the bank.
32013	Phone the bank
32013	Phone the bank for manual authorisation.
32015	Insufficient Funds.
32019	Invalid amount.
32023	Invalid card number
32024	Invalid card number
32027	Invalid expiry date
32032	Invalid budget period
32047	Card has been reported lost
32048	Card has been reported stolen
32049	Card has been reported lost or stolen
32051.1	Unable to connect to the bank
32051.1	Unable to connect to upstream gateway.
32051.1	Unable to connect to the bank
32051.2	Unable to connect to the bank
32051.54	Unable to connect to the bank
32055	Invalid card type.
32057	Incorrect card number
32060	Invalid CVV entered
32062	Restricted card
32063	Connection to the bank timed out
32065	Exceeds withdrawal frequency limit
32068	No PBF (positive balance file)
33006	Unable to process transaction
33009	Duplicate transaction
33012	Invalid transaction
33015	No such issuer
33030	Format error
33031	Bank not supported by switch
33034	Suspected fraud, capture
33035	Card acceptor contact acquirer
33037	Card acceptor call acquirer security. Capture
33057	Transaction not permitted to cardholder
33058	Transaction not permitted to terminal
33062	Number times used
33082	No atalla box

33083	No account connected
33084	No PBF (positive balance file)
33085	PBF update error
33086	Invalid auth type
33088	PTLF (Pos transaction log file) error
33089	Invalid route service
33090	Cutoff is in progress
33092	Financial institution or intermediate network facility cannot be found for routing
33094	Duplicate transmission
33096	System malfunction - unable to process
330N0	Unable to authorize
330N2	Pre auth fail
330N3	Max online refund reached
330N4	Max offline refund reached
330N5	Max credit per refund
330N6	Max refund credit reached
330N7	Customer selected Neg reason
330N8	Over floor limit
330N9	Max number refund credit
330O0	Referral file failed
330O1	Neg file problem
330O2	Advance less than minimum
330O3	Referral file full
330O4	Over limit table
330O5	Pin required
330O6	Mod 10 check
330O7	Force post
330O9	Neg file problem
330P0	CAF (cardholder authorisation file) file problem
330P1	Over daily limit
330P2	CAF (cardholder authorisation positive file) not found
330P3	Advance less than minimum
330P4	Number of times used.
330P5	Delinquent
330P6	Over table limit
330P7	Advance less than minimum
330P8	Admin card needed
330P9	Enter less amount
330Q0	Invalid transaction date
330Q2	Invalid transaction code
330Q3	The merchant account is not configured to accept the payment brand.
330Q3	Advance less than minimum
330Q4	Number of times used
330Q5	Delinquent
330Q6	Over table limit
330Q7	Amount over maximum

330Q8	Admin card not found
330Q9	Admin card not allowed
330R0	Approved admin request / in window
330R1	Approved admin request / out of window
330R2	Approved admin request /any time
330R3	Chargeback / customer file updated
330R4	Chargeback / customer file updated / acquirer not
330R5	Chargeback / incorrect prefix number
330R6	Chargeback / incorrect response code
330R7	Admin transaction not supported
330R8	Card on national negative file
330S4	Ptlf is full
330S7	Accepted, incorrect destination
330S8	Admin file problem
330S9	Unable to validate PIN, security box is down
330T1	Invalid credit card advance increment
330T2	Invalid transaction date
330T3	Card not supported
330T3	Card not supported.
330T4	Amount over maximum
330T5	CAF status 0 or 9
330T6	Bad UAF (usage accumulation file)
330T7	Cash back > daily limit
330T8	Invalid credit card.
330T8	Invalid account or card number.
50841	Insufficient information was provided to approve this payment.
70016	DB file not found
91	Issuer or switch inoperative
B001	Unable to verify merchant
B002	Required field not defined
B003	Merchant not active
B004	Action not valid
B005	Duplicate username
B006	Password and confirm password does not match
B007	General exception error occurred
B008	No profile found for buyer username
B009	Duplicate profiles found for buyer username
B010	Incorrect fields passed for update
B011	30001 Timeout checked by Andre & Bronwyn
B012	32011-05 updated by Bronwyn
B013	32047-41 updated by Bronwyn
B014	Dollar 30006 Timeout updated
B015	Dollar Unknown error updated
Issuer Declined	Your bank has declined your transaction.
T8	Invalid account

WS00025	Member Instrument is loaded but not active.
WS55001	An error occurred and your request could not be completed.
WS55002	No records returned
601	A required field is missing in the transaction request. Invalid transaction type specified in transaction request. Valid values are SHIP,REFUND,CANCEL
602	SHIP,REFUND,CANCEL
603	One or more of the transaction request fields contained invalid data.
604	Login failed. Please ensure that you using the correct username and password.
605	The company or outlet details are incorrect.
606	Outstanding fees on Setcom account. Please contact customer services to your account activated. Order information is incorrect, please ensure you are submitting the correct OrderID and amount.
607	and amount.
608	The order is in a pending state.
609	Please settle this order manually from the Setcom Commerce Manager. Invalid request amount, ensure the amount does not exceed the original authorisation amount.
610	authorisation amount.
611	Error processing refund – error return from bank interface. The credit card has expired. Please obtain the new credit card expiry date and CVV from the buyer.
612	from the buyer.
613	Transaction stopped – invalid card data or order is too old.
614	Invalid OrderID parameter. Merchant account is not active. Please contact customer services to activate your account.
615	account.
616	Invalid order status for required action. Source of transaction not remote interface – only transactions originating from the remote interface can be auctioned remotely.
617	remote interface can be auctioned remotely.
618	The order has been cancelled already.
619	The order has been settled already.
620	The order has not been settled yet. The merchant account terminal configuration is invalid. Please contact customer services.
621	services.
622	The order has already been settled.

## Appendix B - ISO 3166 Country Codes

Please contact customer services if you require the below list in a machine readable format, e.g. CSV (comma-separated-values).

ISO 3166 Code	Country Name
AD	ANDORRA
AE	UNITED ARAB EMIRATES
AF	AFGHANISTAN
AG	ANTIGUA AND BARBUDA
AI	ANGUILLA
AL	ALBANIA
AM	ARMENIA
AN	NETHERLANDS ANTILLES
AO	ANGOLA
AQ	ANTARCTICA
AR	ARGENTINA
AS	AMERICAN SAMOA
AT	AUSTRIA
AU	AUSTRALIA
AW	ARUBA
AX	ÅLAND ISLANDS
AZ	AZERBAIJAN
BA	BOSNIA AND HERZEGOVINA
BB	BARBADOS
BD	BANGLADESH
BE	BELGIUM
BF	BURKINA FASO
BG	BULGARIA
BH	BAHRAIN
BI	BURUNDI
BJ	BENIN
BM	BERMUDA
BN	BRUNEI DARUSSALAM
BO	BOLIVIA
BR	BRAZIL
BS	BAHAMAS
BT	BHUTAN
BV	BOUVET ISLAND
BW	BOTSWANA
BY	BELARUS
BZ	BELIZE
CA	CANADA
CC	COCOS (KEELING) ISLANDS
CD	CONGO (DRC)
CF	CENTRAL AFRICAN REPUBLIC

CG	CONGO
CH	SWITZERLAND
CI	COTE D'IVOIRE
CK	COOK ISLANDS
CL	CHILE
CM	CAMEROON
CN	CHINA
CO	COLOMBIA
CR	COSTA RICA
CS	SERBIA AND MONTENEGRO
CU	CUBA
CV	CAPE VERDE
CX	CHRISTMAS ISLAND
CY	CYPRUS
CZ	CZECH REPUBLIC
DE	GERMANY
DJ	DJIBOUTI
DK	DENMARK
DM	DOMINICA
DO	DOMINICAN REPUBLIC
DZ	ALGERIA
EC	ECUADOR
EE	ESTONIA
EG	EGYPT
EH	WESTERN SAHARA
ER	ERITREA
ES	SPAIN
ET	ETHIOPIA
FI	FINLAND
FJ	FIJI
FK	FALKLAND ISLANDS (MALVINAS)
FM	MICRONESIA (FEDERATED STATES OF)
FO	FAROE ISLANDS
FR	FRANCE
GA	GABON
GB	UNITED KINGDOM
GD	GRENADA
GE	GEORGIA
GF	FRENCH GUIANA
GH	GHANA
GI	GIBRALTAR
GL	GREENLAND
GM	GAMBIA
GN	GUINEA
GP	GUADELOUPE
GQ	EQUATORIAL GUINEA

GR	GREECE
GS	SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS
GT	GUATEMALA
GU	GUAM
GW	GUINEA-BISSAU
GY	GUYANA
HK	HONG KONG
HM	HEARD ISLAND AND MCDONALD ISLANDS
HN	HONDURAS
HR	CROATIA
HT	HAITI
HU	HUNGARY
ID	INDONESIA
IE	IRELAND
IL	ISRAEL
IN	INDIA
IO	BRITISH INDIAN OCEAN TERRITORY
IQ	IRAQ
IR	IRAN
IS	ICELAND
IT	ITALY
JM	JAMAICA
JO	JORDAN
JP	JAPAN
KE	KENYA
KG	KYRGYZSTAN
KH	CAMBODIA
KI	KIRIBATI
KM	COMOROS
KN	SAINT KITTS AND NEVIS
KP	KOREA - DEMOCRATIC PEOPLE'S REPUBLIC OF
KR	KOREA - REPUBLIC OF
KW	KUWAIT
KY	CAYMAN ISLANDS
KZ	KAZAKHSTAN
LA	LAO PEOPLE'S DEMOCRATIC REPUBLIC
LB	LEBANON
LC	SAINT LUCIA
LI	LIECHTENSTEIN
LK	SRI LANKA
LR	LIBERIA
LS	LESOTHO
LT	LITHUANIA
LU	LUXEMBOURG
LV	LATVIA
LY	LIBYAN ARAB JAMAHIRIYA

MA	MOROCCO
MC	MONACO
MD	MOLDOVA
ME	MONTENEGRO
MG	MADAGASCAR
MH	MARSHALL ISLANDS
MK	MACEDONIA
ML	MALI
MM	MYANMAR
MN	MONGOLIA
MO	MACAO
MP	NORTHERN MARIANA ISLANDS
MQ	MARTINIQUE
MR	MAURITANIA
MS	MONTSERRAT
MT	MALTA
MU	MAURITIUS
MV	MALDIVES
MW	MALAWI
MX	MEXICO
MY	MALAYSIA
MZ	MOZAMBIQUE
NA	NAMIBIA
NC	NEW CALEDONIA
NE	NIGER
NF	NORFOLK ISLAND
NG	NIGERIA
NI	NICARAGUA
NL	NETHERLANDS
NO	NORWAY
NP	NEPAL
NR	NAURU
NU	NIUE
NZ	NEW ZEALAND
OM	OMAN
PA	PANAMA
PE	PERU
PF	FRENCH POLYNESIA
PG	PAPUA NEW GUINEA
PH	PHILIPPINES
PK	PAKISTAN
PL	POLAND
PM	SAINT PIERRE AND MIQUELON
PN	PITCAIRN
PR	PUERTO RICO
PS	PALESTINIAN TERRITORY

PT	PORTUGAL
PW	PALAU
PY	PARAGUAY
QA	QATAR
RE	REUNION
RO	ROMANIA
RS	SERBIA
RU	RUSSIAN FEDERATION
RW	RWANDA
SA	SAUDI ARABIA
SB	SOLOMON ISLANDS
SC	SEYCHELLES
SD	SUDAN
SE	SWEDEN
SG	SINGAPORE
SH	SAINT HELENA
SI	SLOVENIA
SJ	SVALBARD AND JAN MAYEN
SK	SLOVAKIA
SL	SIERRA LEONE
SM	SAN MARINO
SN	SENEGAL
SO	SOMALIA
SR	SURINAME
ST	SAO TOME AND PRINCIPE
SV	EL SALVADOR
SY	SYRIAN ARAB REPUBLIC
SZ	SWAZILAND
TC	TURKS AND CAICOS ISLANDS
TD	CHAD
TF	FRENCH SOUTHERN TERRITORIES
TG	TOGO
TH	THAILAND
TJ	TAJIKISTAN
TK	TOKELAU
TL	TIMOR-LESTE
TM	TURKMENISTAN
TN	TUNISIA
TO	TONGA
TR	TURKEY
TT	TRINIDAD AND TOBAGO
TV	TUVALU
TW	TAIWAN
TZ	TANZANIA
UA	UKRAINE
UG	UGANDA

UM	UNITED STATES MINOR OUTLYING ISLANDS
US	UNITED STATES OF AMERICA
UY	URUGUAY
UZ	UZBEKISTAN
VA	HOLY SEE (VATICAN CITY STATE)
VC	SAINT VINCENT AND THE GRENADINES
VE	VENEZUELA
VG	VIRGIN ISLANDS (BRITISH)
VI	VIRGIN ISLANDS (U.S.)
VN	VIET NAM
VU	VANUATU
WF	WALLIS AND FUTUNA
WS	SAMOA
YE	YEMEN
YT	MAYOTTE
ZA	SOUTH AFRICA
ZM	ZAMBIA
ZW	ZIMBABWE

## Appendix C – Programming Samples

Please contact customer services if you do not see your programming language below. We will gladly assist you in getting started with the correct components to use for your language.

### Classic ASP – ASPTear.DLL

Please contact customer services for a copy of ASPTear.DLL. The DLL's sole purpose is to perform HTTP and HTTPS post operations. To install the DLL:

1. Create a new folder and copy the DLL to the newly created folder. For this example lets call the folder `c:\components\asptear\`.
2. Run the following command using the Windows **Run** function or **Command Prompt**:

```
"Regsvr32 c:\components\asptear\asptear.dll"
```

3. Amend your payment code to include the sample code below.

```
Dim Request_POST
Request_POST=1
Set xobj = CreateObject ("SOFTWING.ASPtear")
strRetVal = xobj.Retrieve("https://secure.setcom.co.za/server.cfm",
Request_POST, "CO_ID=" & CO_ID & "&Outlet=" & Outlet & "&Reference=" &
Reference & "&CC_Amount=" & CC_Amount & "&CCname=" & CCname & "&CCnumber=" &
CCnumber & "&CCCVV=" & CCCVV & "&CCtype=" & CCtype & "&ExMonth=" & ExMonth &
"&ExYear=" & ExYear & "&PayPeriod=" & PayPeriod & "&EmailAddress=" &
EmailAddress & "", "", "")
```

4. Use the newly created variable called **strRetVal** to obtain the transaction response.

### .NET Web Application –C# WebRequest method

```
#region Public Properties
public string CO_ID
{
    get;
    set;
}
public string OUTLET
{
    get;
    set;
}
public string Reference
{
    get;
    set;
}
public string CC_Amount
{
    get;
    set;
}
```

```
public string CCName
{
    get;
    set;
}
public string CCNumber
{
    get;
    set;
}
public string CCType
{
    get;
    set;
}
public string ExMonth
{
    get;
    set;
}
public string ExYear
{
    get;
    set;
}
public string PayPeriod
{
    get;
    set;
}
public string CCCVV
{
    get;
    set;
}
public string EmailAddress
{
    get;
    set;
}
#endregion

public static string SampleWebRequest()
{
    try
    {
        #region Test Variable Values
        CO_ID = "testaccount";
        OUTLET = "testaccount";
        Reference = "TEST-001-001";
        CC_Amount = "10.00";
```

```

CCName = "Test";
CCNumber = "4111111111111111"; //"5454545454545454";
CCType = "Visa"; // "MasterCard";
ExMonth = "11"; // "11";
ExYear = "2011"; // "2011";
PayPeriod = "0"; // "0";
CCCVV = "411"; // "545";
EmailAddress = "kyler@setcom.com";
#endregion
#region Request String Builder
StringBuilder builder = new StringBuilder();
builder.Append(string.Format("CO_ID={0}", CO_ID));
builder.Append(string.Format("&Outlet={0}", OUTLET));
builder.Append(string.Format("&Reference={0}", Reference));
builder.Append(string.Format("&CC_Amount={0}", CC_Amount));
builder.Append(string.Format("&CCname={0}", CCName));
builder.Append(string.Format("&CCnumber={0}", CCNumber));
builder.Append(string.Format("&CCCVV={0}", CCCVV));
builder.Append(string.Format("&CCType={0}", CCType));
builder.Append(string.Format("&ExMonth={0}", ExMonth));
builder.Append(string.Format("&ExYear={0}", ExYear));
builder.Append(string.Format("&PayPeriod={0}", PayPeriod));
builder.Append(string.Format("&EmailAddress={0}", EmailAddress));
#endregion
#region Web Requesting
byte[] postData = Encoding.UTF8.GetBytes(builder.ToString());
WebRequest request =
WebRequest.Create("https://secure.setcom.co.za/server.cfm");
request.Method = "POST";
request.ContentType = "application/x-www-form-urlencoded";
request.ContentLength = postData.Length;
Stream data = request.GetRequestStream();
data.Write(postData, 0, postData.Length);
data.Close();
WebResponse response = request.GetResponse();
data = response.GetResponseStream();
StreamReader reader = new StreamReader(data);
#endregion
#region Finalize String
string serverResponse = reader.ReadToEnd();
reader.Close();
string[] TrimStrings = serverResponse.Split(',');
string ReturnString = string.Empty;
for (int i = 0; i < TrimStrings.Length; i++)
{
    if (i != TrimStrings.Length - 1)
        ReturnString = ReturnString + TrimStrings[i].Trim() + ",";
    else
        ReturnString = ReturnString + TrimStrings[i].Trim();
}
#endregion

```

```

        return ReturnString;
    }
catch
{
    return "Error";
}
}

```

## ColdFusion – CFHTTP

ColdFusion has a built-in method to perform HTTP and HTTPS request operations called **CFHTTP**.

```

<CFSET CO_ID = "testaccount">
<CFSET OUTLET = "testaccount">
<CFSET Reference = "PRO0012">
<CFSET CC_Amount = 9.95>
<CFSET CCType = "Visa">
<CFSET CCName = "Mr Test Buyer">
<CFSET CCNumber = "4111111111111111">
<CFSET ExYear = 2015>
<CFSET ExMonth = 11>
<CFSET CCCVV = "411">
<CFSET PayPeriod = 0>
<CFSET EmailAddress = "support@setcom.com">

<CFHTTP METHOD="POST" URL="https://secure.setcom.co.za/server.cfm" TIMEOUT="90">
    <CFHTTPPARAM NAME="CO_ID" VALUE="#CO_ID#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="OUTLET" VALUE="#OUTLET#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="Reference" VALUE="#Reference#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="CC_Amount" VALUE="#CC_Amount#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="CCType" VALUE="#CCType#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="CCName" VALUE="#CCName#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="CCNumber" VALUE="#CCNumber#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="ExYear" VALUE="#ExYear#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="ExMonth" VALUE="#ExMonth#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="CCVV" VALUE="#CCVV#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="PayPeriod" VALUE="#PayPeriod#" TYPE="FORMFIELD">
    <CFHTTPPARAM NAME="EmailAddress" VALUE="#EmailAddress#" TYPE="FORMFIELD">
</CFHTTP>

<CFSET response_message = trim(CFHTTP.FileContent)>

<CFIF listLen(response_message, ",") NEQ 7>
    <CFABORT SHOWERROR="AN ERROR OCCURRED - THE RESPONSE MESSAGE CAN NOT BE
    PARSED.">
</CFELSE>

    <CFSET response_outcome = trim(listGetAt(response_message, 1, ","))>
    <CFSET response_indicator = trim(listGetAt(response_message, 2, ","))>
    <CFSET response_date = trim(listGetAt(response_message, 3, ","))>

    <CFSET response_time = trim(listGetAt(response_message, 4, ","))>
    <CFSET response_reference = trim(listGetAt(response_message, 5, ","))>
    <CFSET response_order_id = trim(listGetAt(response_message, 6, ","))>

```

```
<CFSET response_amount = trim(listGetAt(response_message, 7, ","))>
```

```
<CFSWITCH EXPRESSION="#trim(response_outcome)#">
```

```
<!-- APPROVED -->
```

```
<CFCASE VALUE="APPROVED">
```

```
    Thank you, your purchase has been Approved.
```

```
</CFCASE>
```

```
<!-- DECLINED -->
```

```
<CFCASE VALUE="DECLINED">
```

```
    Sorry, your purchase has been Declined.
```

```
</CFCASE>
```

```
<!-- ERROR -->
```

```
<CFCASE VALUE="ERROR">
```

```
    Sorry, an error occurred while processing your purchase request.
```

```
</CFCASE>
```

```
<!-- STOP -->
```

```
<CFCASE VALUE="STOP">
```

```
    Your order has been stopped by order screening engine. Your card has not  
been charged.
```

```
</CFCASE>
```

```
<!-- REVIEW -->
```

```
<CFCASE VALUE="REVIEW">
```

```
    Your order has been stopped for review by order screening engine. Your card  
has not been charged.
```

```
</CFCASE>
```

```
<!-- ENROLLED -->
```

```
<CFCASE VALUE="ENRIOLLED">
```

```
    <!-- this card is enrolled in secure 3D - redirect buyer to ACS -->
```

```
    <CFLOCATION URL="#trim(response_indicator)#" ADDTOKEN="NO">
```

```
</CFCASE>
```

```
<!-- UNAVAILABLE -->
```

```
<CFCASE VALUE="UNAVAILABLE">
```

```
    Secure 3D authentication is unavailable on your card. Please contact your  
bank is this error persists.
```

```
</CFCASE>
```

```
<!-- ATTEMPTED -->
```

```
<CFCASE VALUE="ATTEMPTED">
```

```
    Secure 3D authentication was attempted on your card, but failed. Please  
contact your bank is this error persists.
```

```
</CFCASE>
```

```
<!-- DUPLICATE -->
```

```
<CFCASE VALUE="DUPLICATE">
```

*This is a duplicate order. Please change the order amount or contact the merchant.*

```

</CFCASE>

<!-- POLL -->
<CFCASE VALUE="POLL">
    <!-- start a polling procedure to poll the order status from the Setcom server
-->
    <CFINCLUDE TEMPLATE="poll_status.cfm">
</CFCASE>

<!-- OTHER -->
<CFDEFAULTCASE>
    <CFABORT SHOWERROR="Your transaction was stopped with a unknown
response. Pelase contact the merchant.">
</CFDEFAULTCASE>

</CFSWITCH>

```

```
</CFIF>
```

## PHP – cURL

The merchant needs to allow and enable the PHP/CURL (php\_curl.dll) extension on the web server before this method will work. For more information on how to enable PHP/CURL for your operating system and web server, please visit the below URL.

<http://www.php.net/manual/en/install.windows.extensions.php>

If the cURL extension is not properly installed on your server, you will receive the following error when trying to run the below sample code.

**Fatal error: Call to undefined function curl\_init() in G:\inetpub\wwwroot\index.php on line 13**

If the cURL extension has been enabled, but you still receive the above error, you will need to restart your web server. Please refer to your web server documentation on how to restart your web server.

The below sample uses PHP/CURL to perform a credit card authorization:

```

<?php

/*
** The function:
*/

function PostRequest($url, $_data) {

    // convert variables array to string:
    $data = array();
    while(list($n,$v) = each($_data)){
        $data[] = "$n=$v";
    }
}

```

```

$dataStr = implode('&', $data);
// format --> test1=a&test2=b etc.

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_PORT, "443");
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $dataStr);
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    $result = curl_exec($ch);

    //close connection
    curl_close($ch);
//    curl_error($ch)
    return $result;
}

// submit these variables to the server:
$data = array(
    'co_id' => $_GET["co_id"],
    'outlet' => $_GET["outlet"],
    'reference' => $_GET["reference"],
    'cc_amount' => $_GET["cc_amount"],
    'ccname' => $_GET["ccname"],
    'ccnumber' => $_GET["ccnumber"],
    'cctype' => $_GET["cctype"],
    'exmonth' => $_GET["exmonth"],
    'exyear' => $_GET["exyear"],
    'payperiod' => $_GET["payperiod"],
    'cccvv' => $_GET["cccvv"],
    'emailaddress' => $_GET["emailaddress"]
);

$setcom_response = PostRequest("https://secure.setcom.co.za/server.cfm",$data);
print_r($setcom_response);
?>

```

The merchant now needs to parse the newly created variable called **\$setcom\_response** and extract the transaction response.

### JSP – HttpURLConnection

```

HttpURLConnection conn = null;
String url = "https://secure.setcom.co.za/server.cfm";
String agent = "Mozilla/4.0";
String rawData =
"CO_ID=testaccount&OUTLET=testaccount&Reference=PRO001&CC_Amount=10.00&CCName=Test

```

```
Buyer&CCNumber=4111111111111111&CCType=Visa&ExYear=2020&ExMonth=11&CCCVV=411&Pa  
yPeriod=0&EmailAddress=email@domain.com";  
String type = "application/x-www-form-urlencoded";
```

```
String encodedData = encode( rawData );
```

```
try {  
    conn = (HttpURLConnection) Connector.open( url );  
    conn.setRequestMethod( HttpURLConnection.POST );  
    conn.setRequestProperty( "User-Agent", agent );  
    conn.setRequestProperty( "Content-Type", type );  
    conn.setRequestProperty( "Content-Length", encodedData.length());  
  
    OutputStream os = conn.getOutputStream();  
    os.write( encodedData.getBytes() );  
  
    int rc = conn.getResponseCode();  
  
    // merchant parse response from setcom  
  
}  
catch( IOException e ){  
    // handle the error here  
}
```

## Contact Information

Please contact us on any of the details below.

<b>Tel:</b>	United Kingdom	+44 20 3051 6320
	United States of America	+1 (408) 850 6530
	South Africa	+27 (83) 913 0000

<b>Fax:</b>	United Kingdom	+44 20 7681 3303
	United States of America	+1 501 643 0401
	South Africa	086 615 1486

**Email:** [support@setcom.co.za](mailto:support@setcom.co.za)

**Web:** [www.setcom.co.za](http://www.setcom.co.za)