

PaymentTrust RiskGuardian



RiskGuardian & PaymentTrust – Implementation Guide



Version: 2.0
April 2007

Copyrights

Copyright 2006, PaymentTrust Limited.

All rights reserved.

Version 2.0

Issue Date: April 2007

Prepared by: PaymentTrust Ltd

Trademarks

Risk Guardian and PaymentTrust logo is trademark or service marks of Payment Trust Limited. All other marks listed in this document may be trademarks of their respective owners and are mentioned for identification purposes only.

This User Manual is protected by the copyright laws and treaties and may not be reproduced without permission from PaymentTrust Limited. You may not use this guide to reverse engineer the PaymentTrust Limited PaymentTrust software.

C Contents

1.	Document Overview.....	1-1
1.1	PURPOSE OF THE DOCUMENT	1-1
1.2	WHO SHOULD READ THIS DOCUMENT	1-1
1.3	TERMINOLOGY.....	1-1
1.4	RELATED DOCUMENTS	1-2
2.	Communication	2-3
2.1	STLINK OVERVIEW	2-3
2.2	NETWORK LAYER	2-5
2.3	SECURITY LAYER.....	2-5
2.4	STLINK APPLICATION	2-5
2.5	NETWORK REQUIREMENTS	2-6
2.6	EXAMPLE REQUEST (STN STRING).....	2-7
2.7	EXAMPLE REQUEST (STN XML).....	2-7
2.8	EXAMPLE XML WITH ESCAPING.....	2-8
2.9	EXAMPLE HTTP POST REQUEST FOR STLINK	2-8
2.10	EXAMPLE HTTP POST REQUEST FOR STLINK BATCH.....	2-8
3.	RiskGuardian	3-9
3.1	RISK GUARDIAN IMPLEMENTATION KEY STAGES.....	3-9
3.2	LOGIC (TSCORE AND TRISK).....	3-10
4.	PaymentTrust.....	4-11
4.1	WHAT IS PAYMENTTRUST?	4-11
4.2	REQUESTYPES	4-11
4.3	PAYMENTTRUST IMPLEMENTATION KEY STAGES	4-12
4.4	METHOD OF PAYMENTS (MOP'S).....	4-12
4.5	STOREIDS.....	4-13
4.6	THE DIFFERENCES WITH DOMESTIC MAESTRO AND SOLO	4-14
4.7	RESPONSE CODES.....	4-14
5.	3D Secure with PaymentTrust	5-17
5.1	WHAT IS 3DSECURE?	5-17
	A TYPICAL 3DSECURE TRANSACTION USING PAYMENTTRUST'S HOSTED MPI.....	5-17
5.2	MERCHANT APPLICATION REQUESTS VIA STLINK FOR 3D SECURE ENROLMENT VERIFICATION. (REQUESTYPE V)	5-17
5.3	ENROLMENT RESPONSE CONTAINS CUSTOMERS ISSUING BANK URL. THE MERCHANT APPLICATION INSTRUCTS CUSTOMER'S BROWSER TO REDIRECT TO THE PROVIDED URL.	5-18
5.4	BROWSER REDIRECTS TO CUSTOMER'S ISSUING BANK URL INCLUDING THE TERMURL AND MD FIELDS. CUSTOMERS ATTEMPT TO AUTHENTICATE THEMSELVES BY ANSWERING THEIR CHALLENGE QUESTION OR ENTERING THEIR PIN.....	5-19

5.5	AUTHENTICATION RESULT IS POSTED BACK TO MERCHANT’S COMMERCE APPLICATION.	5-20
5.6	MERCHANT’S APPLICATION REQUESTS VIA STLINK FOR VALIDITY OF THE AUTHENTICATION RESPONSE. (REQUESTTYPE A).....	5-20
5.7	MERCHANT’S APPLICATION PREPARES A STANDARD AUTH/SALE WITH PROVIDED 3D SECURE FIELDS: ECI, CAV, SECUREID AND SENDS A REQUEST TO STLINK.	5-22
5.8	A RECEIPT PAGE IS RETURNED TO THE CUSTOMER WITH ACCEPTED OR DECLINED MESSAGE.	5-24
6.	Bank Identification Table (BIN) Table	6-25
6.1	SCREENSHOT OF DATA (CSV FORMAT)	6-25
6.2	SCREENSHOT OF DATA (TXT FORMAT)	6-26
7.	URL’s and Tools.....	7-27
	ALL TEST AND LIVE TRANSACTION SYSTEM	7-27
	RG TEST WEBSITE.....	7-27
	PT TEST WEBSITE.....	7-27
8.	Appendix I – RG Set-up Form.....	8-28
9.	Appendix II – PayBack (Credit Card) Set-up Form.....	9-36
10.	Appendix III – PT Acquiring Set-up Form	10-37
11.	Appendix IV – Domestic Maestro and Solo Bins	11-38
12.	Appendix V: message/response codes.....	12-41
13.	Appendix VI: currency codes.....	13-48
14.	Appendix VII: country codes	14-50
15.	Appendix VIII: state/province/region codes.....	15-56
16.	Appendix IX: how to contact us.....	16-59
17.	Glossary of payment processing terminology.....	17-60

1. DOCUMENT OVERVIEW

1.1 Purpose of the Document

This document provides an overview of how to implement PaymentTrust's core services, Risk Guardian and PaymentTrust. Additionally to this there are subsequent documents listed below covering our Payback services and Bank Transfer Service these documents should be read in conjunction with this when implementing these services.

The Developer's guide is the main document for understanding message formats and communication methods.

1.2 Who should read this document

System Integrators and Project Managers responsible for implementing PaymentTrust's products and services.

1.3 Terminology

The following is a glossary of terms and abbreviations used in this document:

Term or Abbreviation	Definition
PT:	PaymentTrust
STLink:	PaymentTrust's Secure Transaction Link
STN:	PaymentTrust's Secure Transaction Network
SSL:	Secure Sockets Layer
API:	Application Program Interface
ASP:	Active Server Pages
CGI:	Common Gateway Interface
VPN:	Virtual Private Network
RG -RM:	RiskGuardian - Risk Management
PT -PP:	PaymentTrust - Payment Processing
Transaction Services	Includes PaymentTrust (PT), RiskGuardian (RG), Bins (BN), Bank Transfer Service (BT), Foreign Exchange (FX), 3DSecure (3D) and others.
Merchant	PaymentTrust Client

1.4 Related Documents

All Integration related documents can be downloaded from the following URL.

<http://www.paymenttrust.ca/devtools/>

PaymentTrust User Guide - PaymentTrust User Guide 2.4.pdf

RiskGuardian User Guide - RiskGuardian User Guide 3.0.pdf

Developer's Guide - MerchantServices-DevGuide-08.20.00.doc

3DSecure Flow Chart - Hosted_MPI_Flow_002 dec06.doc.doc

2. COMMUNICATION

The PaymentTrust Secure Transaction Network (STN) is a collection of robust, multithreaded and real-time transaction systems (See Figure 1 below). STN is composed of the PaymentTrust Secure Transaction Link (STLink) system and back-end Transaction Services. STLink receives transaction information from merchants, processes the information through one of the many transaction services, and sends the response back to the merchant's requesting system. All Internet communication mentioned in this document is executed via an Internet 128 bit Secure Sockets Layer (SSL) connection, or an Internet Virtual Private Network (VPN) connection using the Triple DES standard.

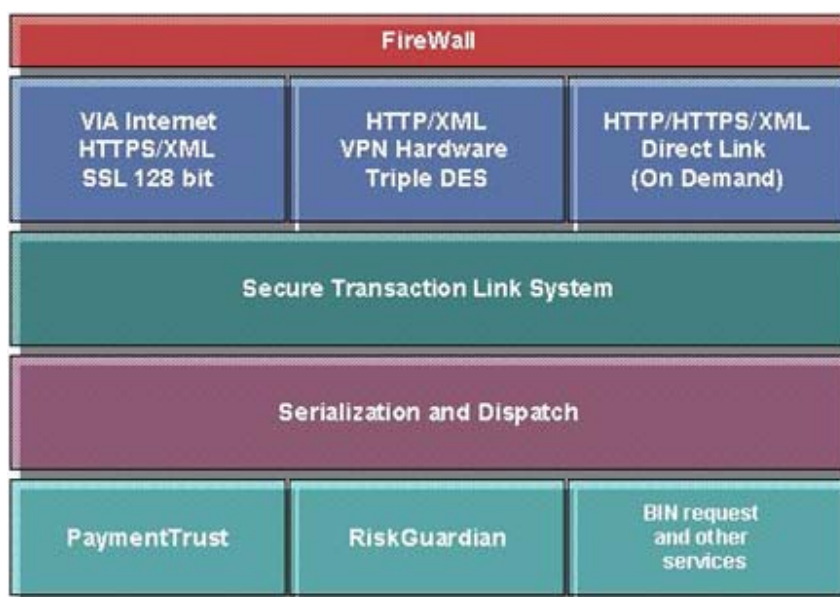


Fig 1: Overview of PaymentTrust's Secure Transaction Network

2.1 STLink Overview

PaymentTrust's Secure Transaction Link (STLink) is a high performance communication solution.

STLink is a service of on-demand secure communication links between the PaymentTrust Secure Transaction Network (STN) and a PaymentTrust Client (Merchant). STLink conforms to encryption and protocol standards as described below (See Figure 2 for network implementation).

Transactions sent between a PaymentTrust Merchant and the PaymentTrust STN travel securely via a 128-bit SSL Internet connection. The STLink system also allows for a hardware encryption method/solution using VPN technology & IPSEC standards.

The Merchant's own application will reside on his system and will be accessible via major web servers, Transaction platforms, and back-end systems. Merchants will be using PaymentTrust's technical specs as guidance to develop their own applications. PaymentTrust provides Merchants example code in ASP/VB, C++, Java, HTML and

XML. Merchants may choose to use their own samples and applications to send transaction information but must conform to the string requirements set in this document.

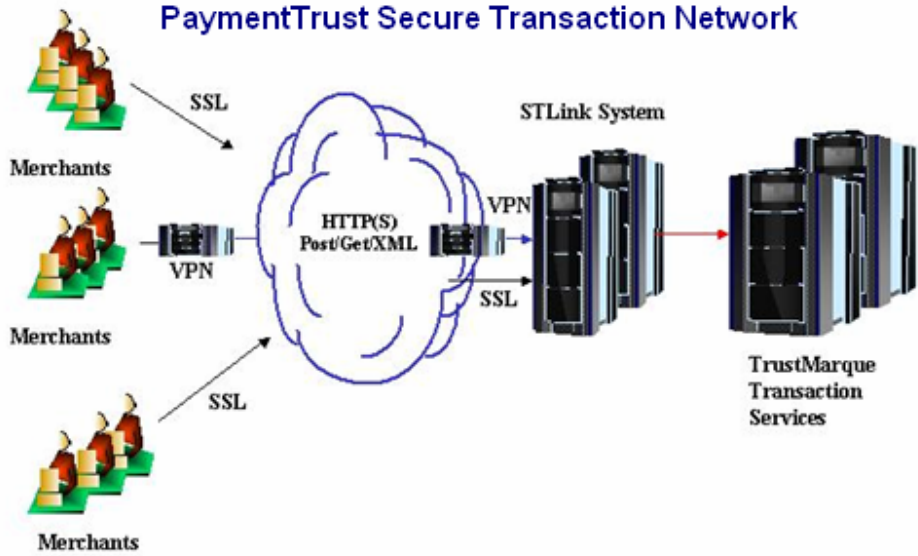
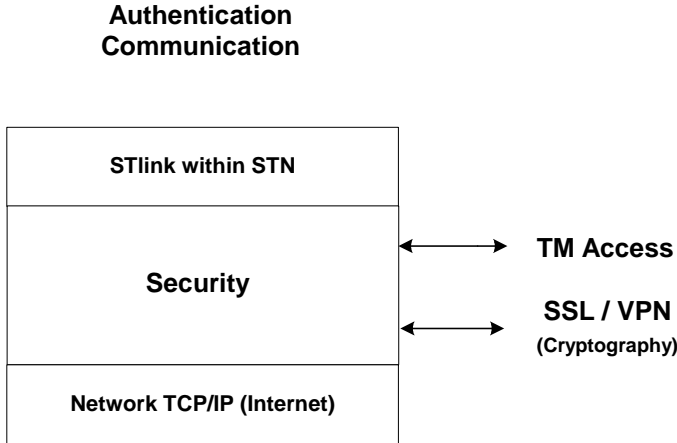


Fig 2: Overview of Network Implementation Possibilities

The STN is comprised of three layers. Descriptions of these layers can be found below in Figure 3.



*** Platform Independent**

Fig. 3 TM Secure Transaction Services Network - Communication Protocol Layers

2.2 Network Layer

This layer is handled exclusively by the designated Internet Service Provider.

2.3 Security Layer

The Security Layer will be handled either by 128 bit SSL certificate or a secure tunnel Triple DES VPN conforming to the IPSEC standard. PaymentTrust will provide at an additional cost the VPN hardware equipment if required.

The Security Layer also includes the Merchant access layer into the PaymentTrust Secure Transaction Network (STN). This involves the use of a Merchant ID, a Username and Password, which are sent as a string to STLink.

2.4 STLink Application

The Application Layer manipulates data using HTTP(S) GET/POST request or an XML request and communicates via standard ports 443 for SSL or port 80 for VPN. The system can intelligently process a request whether GET/POST or XML. The request (an input string) is routed with the STN to the appropriate service for processing – PT, RG, and others. The system returns the response to the requesting URL. Should the delivery fail, the system will capture the error, inform the merchant and store the information for later reporting. Captured errors are further analyzed. When the delivery is successful, the merchant receives a response and stamps each transaction with an appropriate message code. Please note that for larger strings sizes the GET method should not be used.

The input string/message sent by the Merchant is stored in a serialised database with a unique serial number. PaymentTrust maintains a log of any transaction requested by the Merchant and responds with a real-time message which will encapsulate information regarding:

Integrity of the message sent by the Merchant – if a message is received truncated/incomplete or in a tampered condition, the STLink application will capture the error and will respond with the appropriate error message to the merchant's system;

Authentication of sending and receiving agents (attributes that assure a given request is received from a specific trading partner) – messages between Merchant and PaymentTrust must contain attributes that identify and recognize a specific Merchant;

The Type of Transaction requested along with processing statistics. I.e. an RG transaction that took 2 seconds to process from IP NNN.NNN.NNN.NNN using SSL etc.

It must be noted that the STLink system is Payload independent – data within the communication link is independent and can accommodate any type of Transaction, for example, an RG transaction with the same ease as a PT transaction. This eases the transition when new services become available.

The STLink system is based on HTTP/1.1 as a transport protocol as well as XML 1.0. It uses generic protocols for communication between user agents and proxies/gateways and other Internet systems. Communication between a PaymentTrust Merchant and a PaymentTrust STN will be achieved through request

messages and response messages. The STLink system implements and exploits the advantages provided by HTTP(S) and XML.

2.5 Network Requirements

The following is required prior to testing of the STN and STLink system by Merchants.

Internet access or dedicated link into the TMI Secure Transaction Network

The originating external IPs if SSL is used or the internal IP addresses of the computers that will participate in the VPN, as well as the external IP it will use.

Name and phone number of the designated technician or administrator responsible for the integration process.

Notification when the testing process is complete.

Our Network Operations Team will at that point take over of the process. The Merchant will receive the following items from TMI:

VPN hardware if this is the solution chosen.

SSL URL if SSL is chosen (High Encryption Pack).

A merchant must follow a few simple steps to send transactions to the STN.

1. Build the HTTP headers
2. Build the transaction data.
3. Encode the transaction data.
4. Attach the transaction data to the HTTP headers.
5. Open a TCP/IP connection to STN.
6. Establish secure communication to STN using SSL.
7. Send the HTTP request to STN.
8. Receive HTTP response with transaction result from STN.

All transaction requests must be submitted to STLink and all batch requests to STLink Batch in either the STN's string format or as XML documents. Both STLink and STLink Batch accept the HTTP and HTTPS protocols, though it is recommended that the HTTPS protocol be used to safely transmit the requests via the Internet. HTTP is the message protocol used to make request to the STN servers. HTTPS refers to the fact that the HTTP request is done over an encrypted/secure network connection.

The HTTP header should consist of the request method (POST), the requested resource (STLink), the HTTP version (1.1), a new line, the amount of data being posted (Content-Length) and 2 new lines. The 2 new lines at the end of the header allow the separation of the HTTP header from the data being posted.

All requests must be submitted using the HTTP POST method. The POST method works by supplying key/value pairs, where the key and value are split by the "="

symbol and key/value pairs by the “&” symbol. For instance: key1=some value&key2=some value... In the case of STLink, there is one key value pair. The key is StringIn and the value is any of TMI transaction types. The POST data is always attached to the HTTP header after 2 new lines “\n”. An additional 2 new lines must be appended after the POST data to terminate the HTTP request as a whole.

2.6 Example Request (STN String)

This string demonstrates the key value pair of a POST request and contains the data of a partial transaction.

```
StringIn=VersionUsed^1~MerchantId^100000~UserName^Mariah~UserPassword^rr87uy~TransactionType^A~IsTest^1~Timeout^90000~
```

2.7 Example Request (STN XML)

This XML document demonstrates the key value pair of a POST request and contains the data of a partial transaction.

```
StringIn=<?xml
version="1.0"?><TMSTN><VersionUsed>1</VersionUsed><MerchantId>100000</
MerchantId><UserName>Mariah</UserName><UserPassword>rr87uy</UserPasswo
rd><TransactionType>A</TransactionType><IsTest>1</IsTest><Timeout>90000</
Timeout></TMSTN>
```

Though STLink Batch accepts POST requests, it is important to note that the StringIn key is not required and must not be submitted to the STLink Batch for batch requests. If not the batch request will be rejected for reason of being a malformed XML document.

The “=” and “&” symbols are standard characters used in the HTTP protocol to separate key/value pairs, therefore it is important that no “=” and “&” symbols be found in the transactions, although this can be overcome by escaping all characters after the StringIn key by using URL encoding. URL encoding allows the “=”, “&” and other HTTP characters to be included in the transaction.

Example:

```
StringIn=<URL encoded transaction>
```

Because STLink Batch does use the StringIn key, the batch request must not be URL encoded. If not the batch request will be rejected for reason of being a malformed XML document.

XML has its own encoding rules. For one, the STLink and STLink Batch will support any XML document that has been encoded in an 8-bit ANSI character set, such as: ISO-8859-1. Second of all XML has its own share of “special” characters. If any of these characters are to be included within the data of a specified transaction tag, they must be escaped. The table below lists those characters and their escape sequence.

Character	Description	Escape Sequence
<	Less than	<
>	Greater than	>
&	Ampersand	&
'	Single quote	'
"	Double quote	"

2.8 Example XML with escaping

```
<?xml version="1.0"?>
<root>
  <tag1>The text in here contains a less than symbol. Here it is: &lt;</tag1>
  <tag2>The text in here contains a double quote symbol. Here it is: &quot;</tag2>
</root>
```

2.9 Example HTTP POST request for STLink

This shows what an HTTP request to Stlink should be, using the following STN URL: <https://stn01.sectranet.com/stlinkssl/stlink.dll>. \n depicts a new line. The content length is the total amount of bytes including the key pair and the URLEncoded data.

```
POST /stlinkssl/stlink.dll HTTP/1.1\n
Content-Length: 123456\n
\n
StringIn=<URL encoded string or XML document>\n
\n
```

2.10 Example HTTP POST request for STLink Batch

This shows what an HTTP request to Stlink Batch should be, using the following STN URL: <https://stn01.sectranet.com/stlinkssl/stlink.dll>. \n depicts a new line. The content length is the total amount of bytes the XML document.

```
POST /stlinkssl/stlinkbatch.dll HTTP/1.1\n
Content-Length: 123456\n
\n
<XML document with no URLEncoding>\n
\n
```

3. RISKGUARDIAN

RiskGuardian is a secure risk management solution that allows merchants to securely manage the risk associated with doing business on the Internet. RiskGuardian provides a set of static risk factors, determined by TMI, and a set of customizable risk factors, which the merchant can alter to manage their risk on an individual basis.

RG Features:

- Provides risk management and assessment for online transactions
- Total overhead is less than three seconds
- Merchant controlled parameters and values
- Online reporting and administration tools
- Export and Import capabilities for mass updates
- Focused on identity theft through Internet aware as well as traditional parameters
- Over 60 parameters and 300 algorithms and cross checks performed

3.1 *Risk Guardian Implementation key stages*

Technical evaluation

Understanding our API and what impact it will have on your system

Development

Actual coding based on API and system changes required.

Profiling

Understanding the merchant's requirements in terms of blocking lists, previous fraud etc etc. Appendix X is the set-up form for RG where most of this information is obtained.

Testing

Full end to end testing of your application.

Fine Tuning

Sending live data to the Risk Guardian test system for the initial 2 weeks, in order that the risk profile previously completed is 100% in line with the Merchant's requirements. Please note, this is still testing and the logic talked about earlier in this document should be ignored until go-live. Basically, the merchant should not act upon the TScore's until profiling is complete.

Go-live....

3.2 Logic (Tscore and TRisk)

Risk Guardian is works on a scoring basis, 1 meaning an instant pass and 100 meaning an instant failure. Enclosed is a sample transaction.

Request

```
StringIn=VersionUsed^3~MerchantId^100162~OrderNumber^HelpDeskTest~TypeofSale^H~TransactionType^RG~IsTest^1~TimeOut^90000~UserName^umberdella~UserPassword^della~AcctName^EricSmith~MOP^CC~AcctNumber^4000000000000002~ExpDate^092002~CurrencyId^124~Amount^56.78~Title^Mr.~FirstName^Eric~MiddleName^~LastName^Smith~Suffix^3rd~Address1^2130 Gold~Address2^Suite101~Address3^~City^Chicago~StateCode^il~ZipCode^12345-6789~CountryCode^us~PhoneNumber^6188565656~Email^johns@aol.com~ShipToTitle^Mr.~ShipToFirstName^Eric~ShipToMiddleName^~ShipToLastName^Smith~ShipToSuffix^3rd~ShipToAddress1^123Road~ShipToAddress2^~ShipToAddress3^~ShipToCity^Seattle~ShipToStateCode^wa~ShipToZipCode^34567-8907~ShipToCountryCode^us~ShipToPhoneNumber^6188565656~REMOTE_ADDR^205.188.146.23~HTTP_USER_AGENT^MSIE 5.0;WindowsNT~HTTP_ACCEPT_LANGUAGE^en,fr-CA~HTTP_ACCEPT_CHARSET^iso-8859-1,*,utf-8~HTTP_REFERER^www.cnn.com~IsMember^3
```

Response

```
MerchantId^100162~TransactionType^RG~OrderNumber^HelpDeskTest~StrId^1780431~MessageCode^100~GttId^1329853~tScore^100.0000~tRisk^56
```

This transaction scored 100 because the card number is invalid. Please note that transactions can score for a number of reasons i.e. cross reference or velocity controls.

Simply if the TScore is Greater than the TRisk then the transaction had failed your risk profile and shouldn't be processed. By default, if the TScore is equal to or Lower than the TRisk then the transaction should proceed for processing with the acquiring bank either via PaymentTrust or another Payment Processor.

4. PAYMENTTRUST

4.1 What is PaymentTrust?

PaymentTrust is capable of receiving multiple request types within the PT Transaction Type. Each request type instructs the system to perform a different financial transaction. It is important to note that all requests types must follow a logical sequence so prior to a Deposit request one must have an Authorization request. There are cases where the PT TRX is an independent TRX not requiring any other Request type such in the case of a payback TRX or Bank Transfer. Following the submission of a request, the system will return an appropriate response code that will flag the transaction as being either successful, unsuccessful (with reason) or pending (awaiting third party confirmation). Each numeric response code is accompanied by a text definition.

4.2 Requestypes

An Authorization (A) request will reduce the cardholder's open to buy (credit limit). It places a hold on the funds for the merchant with the cardholder's bank for a limited period of time (defined by the credit card associations) before it expires. An authorization does not move any funds to the merchant's bank account. A deposit request type is required to initiate fund collection and is described below.

A Settlement (D) request marks a previously authorized transaction for funds collection during the next deposit cycle with the financial institution. Merchants who do not ship goods immediately should only perform this transaction request at the order fulfillment stage (shipment).

Important Note: A merchant can only submit one deposit request per authorization and this must be for a value lesser or equal to the authorized amount.

A Refund (R) request returns a specified amount to the cardholder's account. The following refund is submitted where a previous deposit transaction has been processed by the system.

Please note that refunds for gaming clients as part of the Visa Credit Funds Transfer programme (CFT) must be sent to PaymentTrust as '**Forced Refunds**'. Details of this Transaction can be found in the Developer's Guide V8.0.16 page 31.

A Simultaneous Authorization and Settlement (S) charges the specified amount against the cardholder's account and marks the transaction for funds collection during the next deposit cycle with the financial institution. This single request initiates both an authorization and a deposit request in the PT system. It should only be used in situations where merchants fulfil their orders immediately. The deposit portion of the 'S' request will only proceed once a successful authorization has been obtained.

A Cancellation (C) - Any transaction that is showing 2050 – request pending can be cancelled.

A Payback (P) request has three methods;

1. Credit card

This is a payment going back to a Credit Card Issuer, quoting the full card number as a reference and is only available to UK issued Mastercard and Visa. Payments are made via BACS Ltd in the UK.

2. Physical Cheque

This is a physical cheque being sent out to the recipient via the conventional post or via courier.

3. Electronic Credit

This is an Electronic payment going back directly to a Clients bank account.

A document entitled 'Payback Service Overview' is available on request which cover the payback service in detail.

A Bank Transfer (B) a document entitled 'Bank Transfer Service Overview' is also available on request.

4.3 PaymentTrust Implementation key stages

Technical evaluation

Understanding our API and what impact it will have on your system.

Development

Actual coding based on API and system changes required.

Testing

Full application end to end testing.

Live bank set-up

Merchant account details are given to the merchant by the Acquiring Bank based on Currency, transaction type, channel (Internet, Moto, digital TV etc), these details are entered into the PaymentTrust live back end systems. Terminal ID's are allocated by PaymentTrust and sent to the Acquiring bank for set-up on their live systems. Once the details are active on both systems then everything is ready and go-live can commence.

Go-live....

4.4 Method of Payments (MOP's)

- CC – Visa and Mastercard credit and debit products (visa credit, visa delta, visa electron, Mastercard Credit, International Maestro)
- DS – Domestic Maestro and Solo
- CQ – Payback via Cheque
- EC – Payback via Electronic Credit
- NT – Neteller
- P2 – Pay2
- DC – PIN enabled debit cards
- PC – Purchasing cards

4.5 StoreIDs

Storeid is mandatory for all TransactionType^PT~. The Storeid is the same number as the Acquiring bank MerchantID. This is required in each transaction in order that PaymentTrust can settle into the correct currency account with the bank.

Typical set-up with Natwest Streamline,

E-commerce sales		Moto sales	
Currency	MerchantID/StoreID	Currency	MerchantID/StoreID
Australian Dollars	64383638	Australian Dollars	52722722
Danish Kroner	81524262	Danish Kroner	26242846
Euro	76494332	Euro	47383563
Euro - Laser Card	42524262	Euro - Laser Card	13252322
Swedish Kronor	22840507	Swedish Kronor	46474647
Swiss Franc's	79585958	Swiss Franc's	53735373
Taiwanese New Dollar (settle in GBP)	63734324	Taiwanese New Dollar (settle in GBP)	72537363
Thai Baht	13538292	Thai Baht	93739383
US Dollars	26836383	US Dollars	83638251
British Pounds	12154121	British Pounds	23262028

E-commerce Refunds		Moto refunds	
Currency	MerchantID/StoreID	Currency	MerchantID/StoreID
Australian Dollars	63836383	Australian Dollars	75857575
Danish Kroner	74846384	Danish Kroner	63736373
Euro	84747498	Euro	98765454
Euro - Laser Card	63736387	Euro - Laser Card	34542872
Hong Kong Dollars	75957595	Hong Kong Dollars	53635396
Swedish Kronor	74948494	Swedish Kronor	25262522
Swiss Franc's	51625171	Swiss Franc's	86323242
Taiwanese New Dollar (settle in GBP)	76584575	Taiwanese New Dollar (settle in GBP)	12415161
Thai Baht	62826282	Thai Baht	86785744
US Dollars	84374847	US Dollars	56252425
British Pounds	23241911	British Pounds	25262526

Typical set-up with Barclaycard Merchant Services,

5464543	Sterling sales
3637363	Sterling refunds
3738373	Multi Currency Sales
8474847	Multi currency refunds

Storeid's for all payback requests is the same as the PaymentTrust Merchant ID ie 100625.

4.6 The Differences with Domestic Maestro and Solo

All Payment Transactions are relevant for switch and solo - Authorisation, Sale, Forced Refund. The difference here is the MOP = DS, the Issuenumber and Startdate. Following fields become mandatory for switch and solo transactions along with all other fields (See the API document for full detailed table);

Field Name	Data Type	Data Size	Description
MOP	Alpha	2	'DS' for Switch/Solo debit cards
Issuenumber	Numeric	2	Issue number stands for the number of cards issued on that bank account. Maximum of 2 digits. The number can be any number between 1 and 99, however normally it's between 1 and 10.
Startdate	Numeric	6	Example "092003"

The additional error codes for switch and solo are;

2280 Incorrect start date congratulations

2282 Invalid issue number

Please note that all switch and solo transaction have to be sent in GBP sterling currency only. CurrencyID = 826.

'Appendix D' shows which switch/ solo card range need an issue number or a start date to process a transaction.

4.7 Response Codes

A full list of response codes can be found in the Developer's guide. Enclosed here is a list of the common response codes.

Payment processing with acquiring bank (Streamline and Barclays)

2100 – Transaction Approved

2200 - Transaction Declined

2958 – Call Acquirer/Issuer

2614 - Acquirer/Issuer Unavailable

2210 – Invalid Credit card number

2212 – Card expired

2644 – Insufficient Terminal ID's

Payback – Credit card

2050 – Request pending (successfully processed, will be processed in next batch)

2223 – No sort code and account number in the payback system

2219 – Not supported the card number is non UK

Please note, for transactions that go on-line in the case of RequestType's A's and S's, if successful the transactions will received a response code 2100 transaction approved. This is also the case for Switch/Solo refunds.

For transactions which are batched and processed at a later time, like refunds R's or payback P's then a successful response is 2050 – request pending.

Switch Refund request example;

Request

StringIn=VersionUsed^1~MerchantId^100625~TransactionType^PT~IsTest^1~Type ofSale^S~TimeOut^90~UserName^TMISUPPORT~UserPassword^tmisupport~Acct Name^Alex~MOP^DS~AcctNumber^4936540000400016~ExpDate^122002~CurrencyId^826~Amount^1.00~RequestType^R~issuenumbr^1~

Response

MerchantId^100625~TransactionType^PT~OrderNumber^5209075289~StrId^8274420~PTTID^10414920~MOP^DS~CurrencyId^826~Amount^1.00~AuthCode^B01637~RequestType^R~MessageCode^2100~Message^Transaction Approved

Visa card Refund request example;

Request

StringIn=VersionUsed^1~MerchantId^100625~TransactionType^PT~IsTest^1~Type ofSale^S~TimeOut^90~UserName^TMISUPPORT~UserPassword^tmisupport~Acct Name^Alex~MOP^cc~AcctNumber^4779160330716625~ExpDate^122005~CurrencyId^826~Amount^1.00~RequestType^R~

Response

MerchantId^100625~TransactionType^PT~OrderNumber^536177545~StrId^8274482~PTTID^10414921~MOP^CC~CurrencyId^826~Amount^1.00~RequestType^R~MessageCode^2050~Message^Request pending

Visa card Authorisation request example;

Request

StringIn=VersionUsed^1~MerchantId^100625~TransactionType^PT~IsTest^1~Type ofSale^S~TimeOut^90~UserName^TMISUPPORT~UserPassword^tmisupport~Acct Name^Alex~MOP^cc~AcctNumber^4779160330716625~ExpDate^122005~CurrencyId^826~Amount^1.00~RequestType^A~

Response

MerchantId^100625~TransactionType^PT~OrderNumber^7470534577~StrId^8274542~PTTID^10414923~MOP^CC~CurrencyId^826~Amount^1.00~AuthCode^B0466F~RequestType^A~MessageCode^2100~Message^Transaction Approved

MasterCard Payback request example;

Request

StringIn=VersionUsed^1~MerchantId^100625~TransactionType^PT~IsTest^1~Type
ofSale^S~TimeOut^90~UserName^TMISUPPORT~UserPassword^tmisupport~Acct
Name^Alex~MOP^cc~AcctNumber^5301207010000012~ExpDate^122005~Currenc
yId^826~Amount^1.00~RequestType^P~Storeid^100625~

Response

MerchantId^100625~TransactionType^PT~OrderNumber^637464746~StrId^827448
2~PTTID^10414967~MOP^CC~CurrencyId^826~Amount^1.00~RequestType^R~M
essageCode^2050~Message^Request pending

5. 3DSECURE WITH PAYMENTTRUST

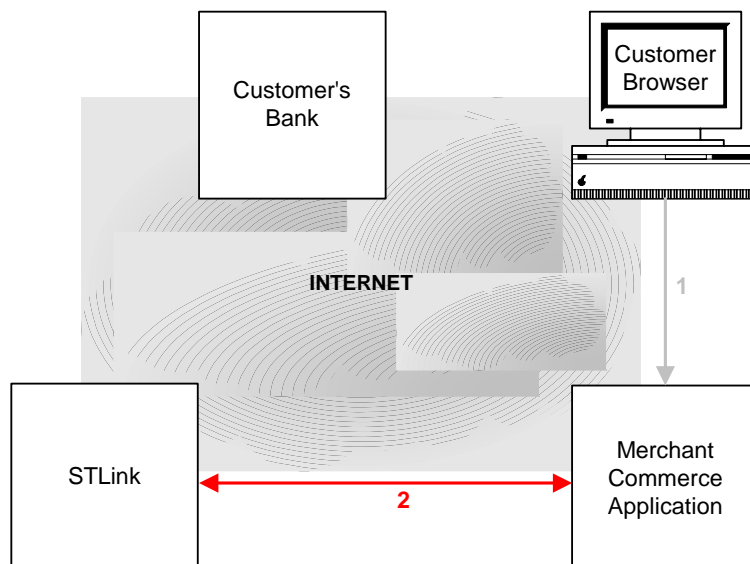
5.1 What is 3DSecure?

3DSecure enables cardholders to authenticate themselves to their issuers through the use of a unique, personal code. It's an industry wide initiative that is being undertaken in order to address current consumer concerns about security of online shopping. This includes Verified By Visa and MasterCard Secure Code.

A Typical 3DSecure Transaction using PaymentTrust's Hosted MPI

Customer confirms his purchase. A form is posted to the merchant's commerce application (php, asp, jsp, cold fusion etc.)

5.2 Merchant application requests via STLink for 3D Secure enrolment verification. (RequestType V)



- a. If enrolment response is successful (CHEnrolled = Y). See Step 5.3.

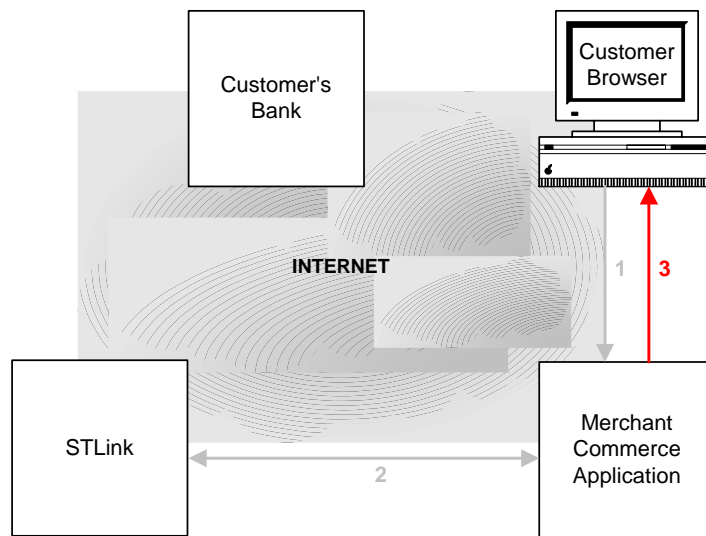
- b. If enrolment verification failed based on the 3D Secure CHEnrolled value, the merchant sends an authorization as follows.

CHEnrolled	VISA	MasterCard
N	Merchant sends authorization request with 3D Secure fields. ECI: 06 CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.	Merchant sends authorization request with 3D Secure fields. ECI: N/A CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.
U	Merchant sends authorization request with 3D Secure fields. ECI: 07 CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.	Merchant sends authorization request with 3D Secure fields. ECI: N/A CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.
N/A	Merchant can decide to send authorization request with 3D Secure fields. ECI: 07 CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.	Merchant can decide to send authorization request with 3D Secure fields. ECI: N/A CAV: N/A. SecureId: SecureId submitted to MPI during enrolment verification. See Step 5.8.

5.3 Enrolment response contains customers issuing bank URL. The merchant application instructs customer's browser to redirect to the provided URL.

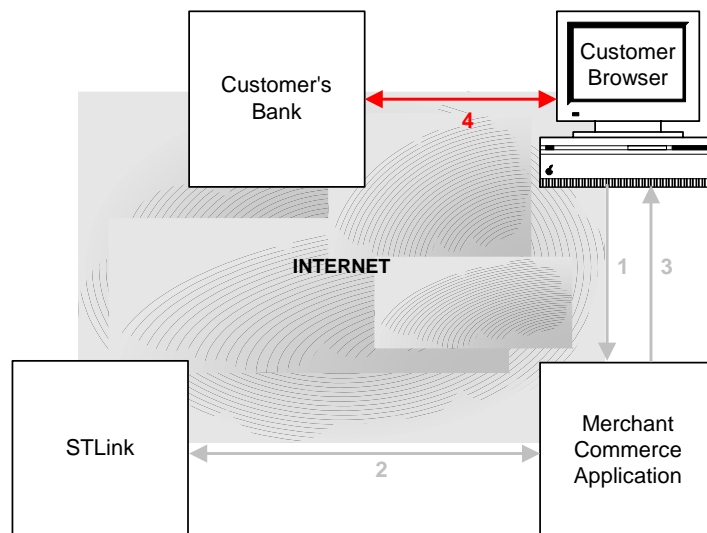
Note 1: This is typically done through hidden form fields and JavaScript that automatically posts the form to the bank URL.

Note 2: The merchant session is re-established as follows. When the merchant application instructs the browser to redirect, there are 2 hidden form fields TermUrl and MD (Merchant Data). The TermUrl tells the issuing bank where to POST back the results. The MD field may contain any value the merchant may require to establish back the session. Before placing any sensitive data in the MD field it must be encrypted.



See Step 5.4.

5.4 Browser redirects to customer's issuing bank URL including the TermUrl and MD fields. Customers attempt to authenticate themselves by answering their challenge question or entering their pin

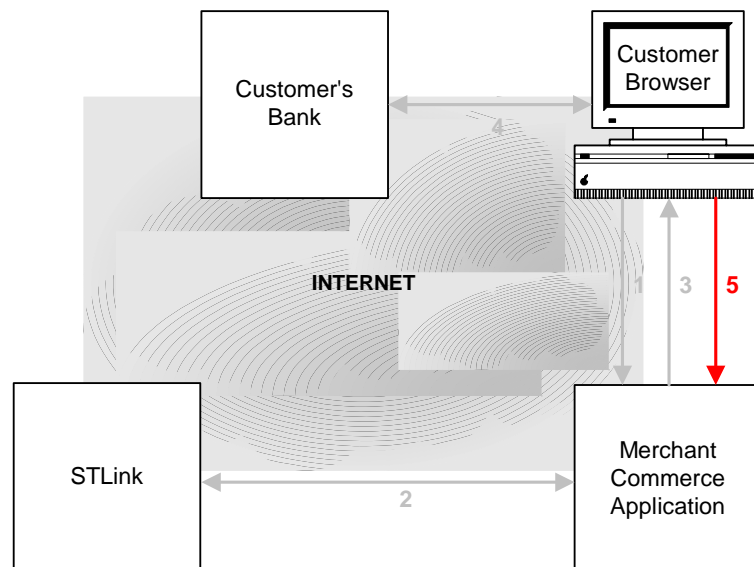


See Step 5.5.

5.5 Authentication result is posted back to merchant's commerce application.

Note 1: In Step 5.3, one of the hidden form fields (TermUrl) contains a merchant assigned URL that is used to receive the authentication response.

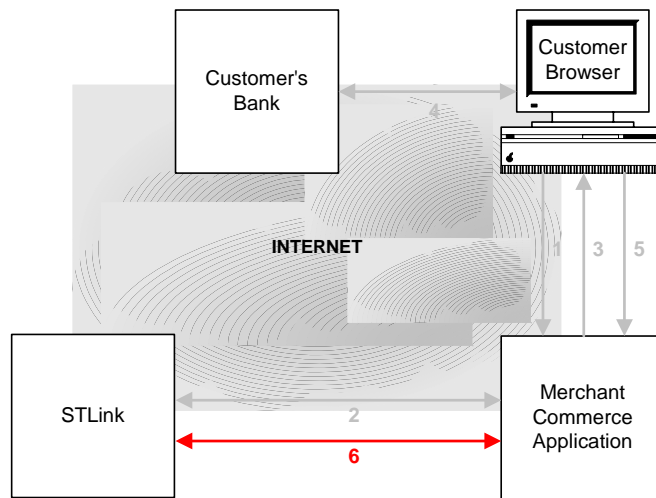
Note 2: The MD field will also be posted back as a hidden form field. This is the data the merchant opted to include during Step 5.3.



See Step 5.6.

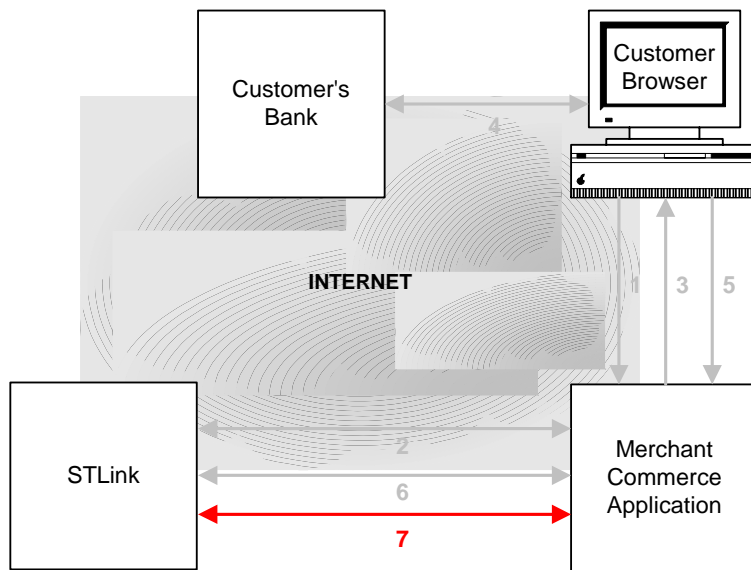
5.6 Merchant's application requests via STLink for validity of the authentication response. (RequestType A)

- a) If authentication succeeded (customer answered challenge correctly). See Step 5.7.
- b) If authentication failed based on the 3D Secure TXStatus value, the merchant may be able to send an authorization.



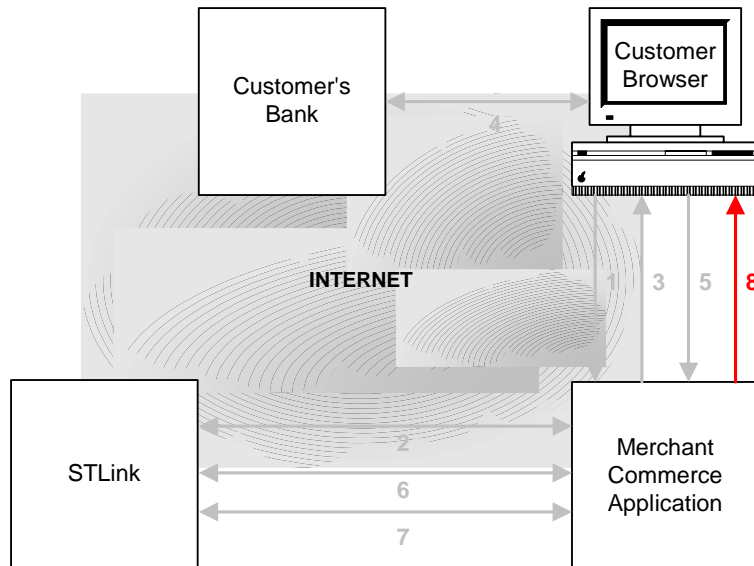
TXStatus	VISA	MasterCard
N	Merchant must not send authorization and decline customer's purchase. See Step 5.8.	Merchant must not send authorization and decline customer's purchase. See Step 5.8.
A	Merchant sends authorization request with 3D Secure fields. ECI: 06 CAV: Send if available. Secureld: Secureld submitted to MPI during enrolment verification. See Step 5.8.	Merchant sends authorization request with 3D Secure fields. ECI: 01 CAV: Send if available. Secureld: Secureld submitted to MPI during enrolment verification. See Step 5.8.
U	Merchant can decide to send authorization. ECI: 07 CAV: N/A. Secureld: Secureld submitted to MPI during enrolment verification. See Step 5.8.	Merchant can decide to send authorization. ECI: N/A CAV: N/A. Secureld: Secureld submitted to MPI during enrolment verification. See Step 5.8.
N/A	Merchant must not send authorization and decline customer's purchase. See Step 5.8.	Merchant must not send authorization and decline customer's purchase. See Step 5.8.

5.7 Merchant's application prepares a standard auth/sale with provided 3D Secure fields: ECI, CAV, Secureld and sends a request to STLink.



TXStatus	VISA	MasterCard
Y	Merchant sends authorization request with 3D Secure fields. ECI: 05 CAV: Send if available. SecureId: SecureId submitted to MPI during enrolment verification. See Step 8.	Merchant sends authorization request with 3D Secure fields. ECI: 02 CAV: Send if available. SecureId: SecureId submitted to MPI during enrolment verification. See Step 8.

5.8 A receipt page is returned to the customer with accepted or declined message.



6. BANK IDENTIFICATION TABLE (BIN) TABLE

To download the latest BIN table go to the following URL

<https://www.trustmarque.ca/Paymenttrust1.2-Live/BINSDownload/>

And type in the username and password (If asked), below;

Username: support

Password:tmicsupport

Right click on tmibin.csv

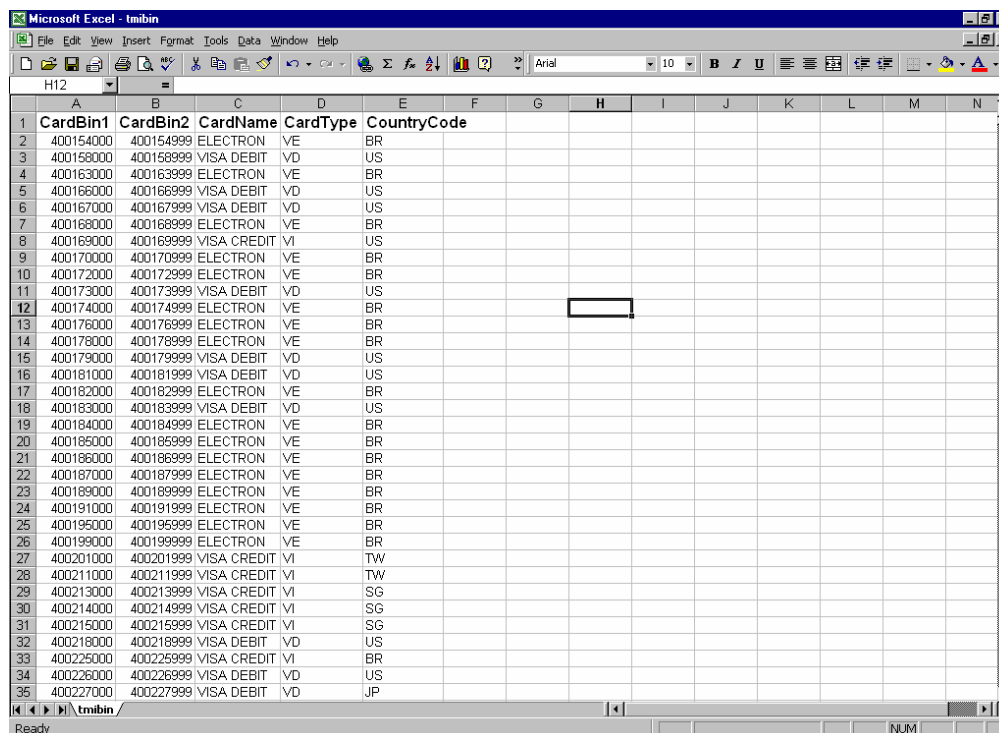
A pop up window appears click on save

Change the file extension from **csv** to **txt** and then click save to your desired location.

It will take approximately 4 minutes to download and will be a 7 MB file. The BIN table may be downloaded as often as required. PaymentTrust will update the table weekly on a Wednesday, at 8.00am GMT. PaymentTrust will erase all BINs on this day and upload the new table from NatWest. Therefore there is no update just a complete replace.

6.1 Screenshot of data (csv format)

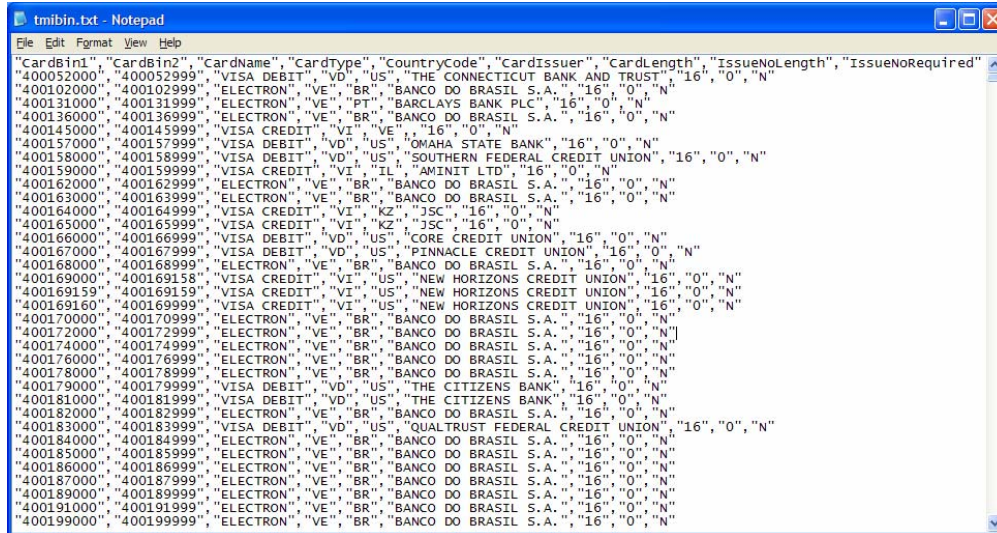
Below is a screenshot showing the fields of data provided. The list is CardBIN1, CardBin2, CardName, CardType and CountryCode.



The screenshot shows a Microsoft Excel spreadsheet with the following data:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	CardBin1	CardBin2	CardName	CardType	CountryCode									
2	400154000	400154999	ELECTRON	VE	BR									
3	400156000	400156999	VISA DEBIT	VD	US									
4	400163000	400163999	ELECTRON	VE	BR									
5	400166000	400166999	VISA DEBIT	VD	US									
6	400167000	400167999	VISA DEBIT	VD	US									
7	400168000	400168999	ELECTRON	VE	BR									
8	400169000	400169999	VISA CREDIT	VI	US									
9	400170000	400170999	ELECTRON	VE	BR									
10	400172000	400172999	ELECTRON	VE	BR									
11	400173000	400173999	VISA DEBIT	VD	US									
12	400174000	400174999	ELECTRON	VE	BR									
13	400176000	400176999	ELECTRON	VE	BR									
14	400178000	400178999	ELECTRON	VE	BR									
15	400179000	400179999	VISA DEBIT	VD	US									
16	400181000	400181999	VISA DEBIT	VD	US									
17	400182000	400182999	ELECTRON	VE	BR									
18	400183000	400183999	VISA DEBIT	VD	US									
19	400184000	400184999	ELECTRON	VE	BR									
20	400185000	400185999	ELECTRON	VE	BR									
21	400186000	400186999	ELECTRON	VE	BR									
22	400187000	400187999	ELECTRON	VE	BR									
23	400189000	400189999	ELECTRON	VE	BR									
24	400191000	400191999	ELECTRON	VE	BR									
25	400195000	400195999	ELECTRON	VE	BR									
26	400199000	400199999	ELECTRON	VE	BR									
27	400201000	400201999	VISA CREDIT	VI	TW									
28	400211000	400211999	VISA CREDIT	VI	TW									
29	400213000	400213999	VISA CREDIT	VI	SG									
30	400214000	400214999	VISA CREDIT	VI	SG									
31	400215000	400215999	VISA CREDIT	VI	SG									
32	400218000	400218999	VISA DEBIT	VD	US									
33	400225000	400225999	VISA CREDIT	VI	BR									
34	400226000	400226999	VISA DEBIT	VD	US									
35	400227000	400227999	VISA DEBIT	VD	JP									

6.2 Screenshot of data (txt format)



```
tmibin.txt - Notepad
File Edit Format View Help
"CardBin1" "CardBin2" "CardName" "CardType" "CountryCode" "CardIssuer" "CardLength" "IssueNoLength" "IssueNoRequired"
"400052000" "400052999" "VISA DEBIT" "VD" "US" "THE CONNECTICUT BANK AND TRUST" "16" "0" "N"
"400102000" "400102999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400131000" "400131999" "ELECTRON" "VE" "PT" "BARCLAYS BANK PLC" "16" "0" "N"
"400136000" "400136999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400145000" "400145999" "VISA CREDIT" "VI" "VE" "16" "0" "N"
"400157000" "400157999" "VISA DEBIT" "VD" "US" "OMAHA STATE BANK" "16" "0" "N"
"400158000" "400158999" "VISA DEBIT" "VD" "US" "SOUTHERN FEDERAL CREDIT UNION" "16" "0" "N"
"400159000" "400159999" "VISA CREDIT" "VI" "IL" "AMINIT LTD" "16" "0" "N"
"400162000" "400162999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400163000" "400163999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400164000" "400164999" "VISA CREDIT" "VI" "KZ" "JSC" "16" "0" "N"
"400165000" "400165999" "VISA CREDIT" "VI" "KZ" "JSC" "16" "0" "N"
"400166000" "400166999" "VISA DEBIT" "VD" "US" "CORE CREDIT UNION" "16" "0" "N"
"400167000" "400167999" "VISA DEBIT" "VD" "US" "PINNACLE CREDIT UNION" "16" "0" "N"
"400168000" "400168999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400169000" "400169158" "VISA CREDIT" "VI" "US" "NEW HORIZONS CREDIT UNION" "16" "0" "N"
"400169159" "400169159" "VISA CREDIT" "VI" "US" "NEW HORIZONS CREDIT UNION" "16" "0" "N"
"400169160" "400169999" "VISA CREDIT" "VI" "US" "NEW HORIZONS CREDIT UNION" "16" "0" "N"
"400170000" "400170999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400172000" "400172999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400174000" "400174999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400176000" "400176999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400178000" "400178999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400179000" "400179999" "VISA DEBIT" "VD" "US" "THE CITIZENS BANK" "16" "0" "N"
"400181000" "400181999" "VISA DEBIT" "VD" "US" "THE CITIZENS BANK" "16" "0" "N"
"400182000" "400182999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400183000" "400183999" "VISA DEBIT" "VD" "US" "QUALTRUST FEDERAL CREDIT UNION" "16" "0" "N"
"400184000" "400184999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400185000" "400185999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400186000" "400186999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400187000" "400187999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400189000" "400189999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400191000" "400191999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
"400199000" "400199999" "ELECTRON" "VE" "BR" "BANCO DO BRASIL S.A." "16" "0" "N"
```

7. URL'S AND TOOLS

All Test and Live transaction system

Primary

<https://stn01.sectranet.com/stlinkssl/stlink.dll?>

<https://stn01.sectranet.com/stlinkssl/stlinkbatch.dll?> (Batch)

Secondary

<https://stl007.kontek.cc/stlinkssl/stlink.dll?>

<https://stl007.kontek.cc/stlinkssl/stlinkbatch.dll?> (Batch)

RG Test website

<https://merchantadmin.riskguardian.com/test/>

PT Test website

<https://merchantadmin.paymenttrust.com/test/>

8. APPENDIX I – RG SET-UP FORM

<u>PaymentTrust Ltd</u> <u>Sales Representative</u>	<u>Date</u>	<u>PaymentTrust Ltd</u> <u>Identifier (PTMID)</u>
--	-------------	--

Product Profile:

What products are sold?

Do you provide hard, digital or service goods?

Please provide details of accepted currencies and associated values.

<u>Currency:</u>	<u>Avg Sale</u>	<u>Highest Sale</u>	<u>Lowest Sale</u>

Are the majority of sales to male or females?

How often will a consumer buy on average?

Do you require the consumer to register?

Will registration i.e. length of membership be passed to RG?

Do you require consumers to use a wallet/account?

How long does it take to refill the wallet/account: _____

Have you experienced any fraud problems? Please provide details below _____

<i>Country</i>	<i>Country Code</i>	<i>Which countries do you sell to?</i>	<i>Which countries do you not wish to sell to?</i>	<i>Which countries have you experienced problems?</i>
Algeria	DZ			
American Samoa	AS			
Andorra	AD			
Angola	AO			
Anguilla	AI			
Antarctica	AQ			
Antigua and Barbuda	AG			
Argentina	AR			
Armenia	AM			
Aruba	AW			
Australia	AU			
Austria	AT			
Azerbaijan	AZ			
Bahamas	BS			
Bahrain	BH			
Bangladesh	BD			
Barbados	BB			
Belarus	BY			
Belgium	BE			
Belize	BZ			
Benin	BJ			
Bermuda	BM			
Bhutan	BT			
Bolivia	BO			
Bosnia and Herzegovina	BA			
Botswana	BW			
Bouvet Island	BV			

Brazil	BR			
British Indian Ocean Territory	IO			
Brunei Darussalam	BN			
Bulgaria	BG			
Burkina Faso	BF			
Burundi	BI			
Cambodia	KH			
Cameroon	CM			
Canada	CA			
Cape Verde	CV			
Cayman Islands	KY			
Central African Republic	CF			
Chad	TD			
Chile	CL			
China	CN			
Christmas Island (Australia)	CX			
Cocos (Keeling) Islands	CC			
Colombia	CO			
Comoros	KM			
Congo	CG			
Cook Islands	CK			
Costa Rica	CR			
Cote D'Ivoire (Ivory Coast)	CI			
Croatia (Hrvatska)	HR			
Cuba	CU			
Cyprus	CY			
Czech Republic	CZ			
Denmark	DK			
Djibouti	DJ			
Dominica	DM			
Dominican Republic	DO			

East Timor	TP			
Ecuador	EC			
Egypt	EG			
El Salvador	SV			
Equatorial Guinea	GQ			
Eritrea	ER			
Estonia	EE			
Ethiopia	ET			
Faeroe Islands	FO			
Falkland Islands (Malvinas)	FK			
Fiji	FJ			
Finland	FI			
France	FR			
French Guiana	GF			
French Polynesia	PF			
Gabon	GA			
Gambia	GM			
Georgia	GE			
Germany	DE			
Ghana	GH			
Gibraltar	GI			
Great Britain	GB			
Greece	GR			
Greenland	GL			
Grenada	GD			
Guadeloupe	GP			
Guam	GU			
Guatemala	GT			
Guinea	GN			
Guinea Bissau	GW			
Guyana	GY			
Haiti	HT			
Honduras	HN			
Hong Kong	HK			
Hungary	HU			
Iceland	IS			
India	IN			
Indonesia	ID			
Iran	IR			
Iraq	IQ			
Ireland	IE			

Isle of Man (U.K.)	IM			
Israel	IL			
Italy	IT			
Jamaica	JM			
Japan	JP			
Johnston Island	JT			
Jordan	JO			
Kazakhstan	KZ			
Kenya	KE			
Kiribati	KI			
Korea (North)	KP			
Korea (South)	KR			
Kuwait	KW			
Kyrgyzstan	KG			
Lao P.Dem.R.	LA			
Latvia	LV			
Lebanon	LB			
Lesotho	LS			
Liberia	LR			
Libyan Arab Jamahiriya	LY			
Liechtenstein	LI			
Lithuania	LT			
Luxembourg	LU			
Macau	MO			
Macedonia	MK			
Madagascar	MG			
Malawi	MW			
Malaysia	MY			
Maldives	MV			
Mali	ML			
Malta	MT			
Marshall Islands	MH			
Martinique	MQ			
Mauritania	MR			
Mauritius	MU			
Mexico	MX			
Micronesia	FM			
Midway Islands	MI			
Moldova	MD			
Monaco	MC			

Mongolia	MN			
Montserrat	MS			
Morocco	MA			
Mozambique	MZ			
Myanmar	MM			
Namibia	NA			
Nauru	NR			
Nepal	NP			
Netherlands	NL			
Netherlands Antilles	AN			
New Caledonia	NC			
New Zealand	NZ			
Nicaragua	NI			
Niger	NE			
Nigeria	NG			
Niue	NU			
Norfolk Island	NF			
Northern Mariana Islands	MP			
Norway	NO			
Oman	OM			
Pakistan	PK			
Palau	PW			
Panama	PA			
Papua New Guinea	PG			
Paraguay	PY			
Peru	PE			
Philippines	PH			
Pitcairn	PN			
Poland	PL			
Portugal	PT			
Puerto Rico	PR			
Qatar	QA			
Reunion	RE			
Romania	RO			
Russian Federation	RU			
Rwanda	RW			
Saint Helena	SH			
Saint Kitts and Nevis	KN			
Saint Lucia	LC			

Saint Pierre and Miquelon	PM			
Saint Vincent and The Grenadines	VC			
Samoa	WS			
San Marino	SM			
Sao Tome and Principe	ST			
Saudi Arabia	SA			
Senegal	SN			
Seychelles	SC			
Sierra Leone	SL			
Singapore	SG			
Slovakia	SK			
Slovenia	SI			
Solomon Islands	SB			
Somalia	SO			
South Africa	ZA			
Spain	ES			
Sri Lanka	LK			
Sudan	SD			
Suriname	SR			
Svalbard and Jan Mayen Islands	SJ			
Swaziland	SZ			
Sweden	SE			
Switzerland	CH			
Syrian Arab Rep.	SY			
Taiwan	TW			
Tajikistan	TJ			
Tanzania	TZ			
Thailand	TH			
Togo	TG			
Tokelau	TK			
Tonga	TO			
Trinidad and Tobago	TT			
Tunisia	TN			
Turkey	TR			
Turkmenistan	TM			
Turks and	TC			

Caicos Islands				
Tuvalu	TV			
Uganda	UG			
Ukraine	UA			
United Arab Emirates	AE			
United States	US			
Uruguay	UY			
Uzbekistan	UZ			
Vanuatu	VU			
Vatican City State (Holy See)	VA			
Venezuela	VE			
Viet Nam	VN			
Virgin Islands (British)	VG			
Virgin Islands (US)	VI			
Wake Island	WK			
Wallis and Futuna Islands	WF			
Western Sahara	EH			
Yemen	YE			
Yugoslavia	YU			
Zaire	ZR			
Zambia	ZM			
Zimbabwe	ZW			

9. APPENDIX II – PAYBACK (CREDIT CARD) SET-UP FORM

Merchant Name

.....

Bank Sort Code

.....

Account Number

.....

File Name

.....

BACS User Number

.....

Originator's Reference

.....PaymentTrust.....

..

10. APPENDIX III – PT ACQUIRING SET-UP FORM

<u>PaymentTrust Ltd</u> <u>Sales Representative</u>	<u>Date</u>	<u>PaymentTrust Ltd</u> <u>Identifier (TMID)</u>

Merchant Acquiring Bank Name _____

Merchant ID: _____

Credit & Debit Cards Accepted²

Visa	<input type="checkbox"/>	
Visa (Purchasing)	<input type="checkbox"/>	
Master Card	<input type="checkbox"/>	
Maestro	<input type="checkbox"/>	
JCB	<input type="checkbox"/>	
Switch/ Solo	<input type="checkbox"/>	
Delta	<input type="checkbox"/>	
Electron	<input type="checkbox"/>	
American Express *	<input type="checkbox"/>	

*American Express/Diners separate authorisations are required for these credit cards see PPD for latest information

Trading Currencies

Please list all the currencies that you currently trade in.

Currencies:

11. APPENDIX IV – DOMESTIC MAESTRO AND SOLO BINS

CardBin1	CardBin2	Card Name	Card Type	Country Code	CardIssuer	Card Length	IssueNo Length	IssueNo Required	StartDate Required
633300000	633300999	SWITCH	SW	GB	HSBC	16	0	N	Y
633301000	633301999	SWITCH	SW	GB	YORKSHIRE BANK	19	1	Y	N
633302000	633302999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633303000	633303999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633304000	633304999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633311000	633311999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
633312000	633312999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633450000	633450999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
633451000	633451999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
633452000	633452999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
633453000	633453999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
633454000	633454999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633455000	633455999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633456000	633456999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633457000	633457999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
633461000	633461999	SOLO	SW	GB	HSBC	18	1	Y	N
633473000	633473999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
633476000	633476999	SOLO	SW	GB	YORKSHIRE BANK	19	1	Y	N
633478000	633478999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
633481000	633481999	SOLO	SW	GB	YORKSHIRE BANK	19	1	Y	N
633490000	633490999	SOLO	SW	GB	BANK OF SCOTLAND	16	1	Y	N
633491000	633491999	SOLO	SW	GB	BANK OF SCOTLAND	16	1	Y	N
633492000	633492999	SOLO	SW	GB	BANK OF SCOTLAND	16	1	Y	N
633493000	633493999	SOLO	SW	GB	BANK OF SCOTLAND	16	1	Y	N
633494000	633494999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
633495000	633495999	SOLO	SW	GB	HALIFAX	16	2	Y	N
633496000	633496999	SOLO	SW	GB	HALIFAX	16	2	Y	N
633497000	633497999	SOLO	SW	GB	HALIFAX	16	2	Y	N
633498000	633498999	SOLO	SW	GB	NATWEST	19	1	Y	N
633499000	633499999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
671850000	671850999	SWITCH	SW	GB			0	N	Y
671851000	671851999	SWITCH	SW	GB			0	N	Y
671852000	671852999	SWITCH	SW	GB			0	N	Y
671853000	671853999	SWITCH	SW	GB			0	N	Y
671854000	671854999	SWITCH	SW	GB			0	N	Y
671855000	671855999	SWITCH	SW	GB			0	N	Y
671856000	671856999	SWITCH	SW	GB			0	N	Y
675901000	675901999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675905000	675905999	SWITCH	SW	GB	YORKSHIRE BANK	19	1	Y	N

675906000	675906999	SWITCH	SW	GB	HALIFAX	16	0	N	Y
675907000	675907999	SWITCH	SW	GB	HALIFAX	16	0	N	Y
675908000	675908999	SWITCH	SW	GB	HALIFAX	16	0	N	Y
675909000	675909999	SWITCH	SW	GB	HALIFAX	16	0	N	Y
675910000	675910999	SWITCH	SW	GB	HALIFAX	16	0	N	Y
675918000	675918999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675938000	675938999	SWITCH	SW	GB	HSBC	18	1	Y	N
675939000	675939999	SWITCH	SW	GB	HSBC	18	1	Y	N
675940000	675940999	SWITCH	SW	GB	HSBC	18	1	Y	N
675950000	675950999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675951000	675951999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675952000	675952999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675953000	675953999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675954000	675954999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675955000	675955999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675956000	675956999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675957000	675957999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675958000	675958999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675959000	675959999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675960000	675960999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675961000	675961999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675962000	675962999	SWITCH	SW	GB	NATWEST	19	1	Y	N
675963000	675963999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675964000	675964999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675965000	675965999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675966000	675966999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675967000	675967999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675968000	675968999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675969000	675969999	SWITCH	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
675970000	675970999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
675971000	675971999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
675972000	675972999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
675973000	675973999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
675982000	675982999	SWITCH	SW	GB	CLYDESDALE BANK PLC	16	0	N	Y
675995000	675995999	SWITCH	SW	GB	CLYDESDALE BANK PLC	16	0	N	Y
675996000	675996999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
675998000	675998999	SWITCH	SW	GB	NATWEST	19	1	Y	N
676701000	676701999	SOLO	SW	GB	NATWEST	19	1	Y	N
676703000	676703999	SOLO	SW	GB	HSBC	18	1	Y	N
676705000	676705999	SOLO	SW	GB	YORKSHIRE BANK	19	1	Y	N
676706000	676706999	SOLO	SW	GB	HALIFAX	16	2	Y	N
676707000	676707999	SOLO	SW	GB	HALIFAX	16	2	Y	N
676708000	676708999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
676709000	676709999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y

676710000	676710999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
676711000	676711999	SOLO	SW	GB	ROYAL BANK OF SCOTLAND	16	0	N	Y
676712000	676712999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
676713000	676713999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
676714000	676714999	SWITCH	SW	GB	BANK OF SCOTLAND	16	0	N	Y
676715000	676715999	SOLO	SW	GB	BANK OF SCOTLAND	16	0	N	Y
676718000	676718999	SOLO	SW	GB	NATWEST	19	1	Y	N
676740000	676740999	SOLO	SW	GB	HSBC	18	1	Y	N
676750000	676750999	SOLO	SW	GB	NATWEST	19	1	Y	N
676751000	676751999	SOLO	SW	GB	NATWEST	19	1	Y	N
676752000	676752999	SOLO	SW	GB	NATWEST	19	1	Y	N
676753000	676753999	SOLO	SW	GB	NATWEST	19	1	Y	N
676754000	676754999	SOLO	SW	GB	NATWEST	19	1	Y	N
676755000	676755999	SOLO	SW	GB	NATWEST	19	1	Y	N
676756000	676756999	SOLO	SW	GB	NATWEST	19	1	Y	N
676757000	676757999	SOLO	SW	GB	NATWEST	19	1	Y	N
676758000	676758999	SOLO	SW	GB	NATWEST	19	1	Y	N
676759000	676759999	SOLO	SW	GB	NATWEST	19	1	Y	N
676760000	676760999	SOLO	SW	GB	NATWEST	19	1	Y	N
676761000	676761999	SOLO	SW	GB	NATWEST	19	1	Y	N
676762000	676762999	SOLO	SW	GB	NATWEST	19	1	Y	N
676770000	676770999	SOLO	SW	GB	YORKSHIRE BANK	19	1	Y	N
676774000	676774999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
676779000	676779999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
676782000	676782999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
676795000	676795999	SOLO	SW	GB	CLYDESDALE BANK PLC	18	1	Y	N
676798000	676798999	SOLO	SW	GB	NATWEST	19	1	Y	N

12. APPENDIX V: MESSAGE/RESPONSE CODES

The following list reflects all currently defined RiskGuardian response codes. One of the following codes is returned with each transaction that is submitted into the RiskGuardian system. Many of these codes will never be returned in your output.

Message Code	Description
100	Ok
200	Transaction does not exist
300	Field(s) Missing (Basic)
301	Field(s) Missing (Transaction Specific)
302	Wrong MerchantId, User Name or Password
303	DB/System undefined errors or packet loss during transmission - Please send again
304	Time out during Transmission - Please send again
305	HTTP(S) method not supported – Please call support
306	Batch Transmission Error - Failed to write to file
307	Invalid document or Wrong XML Format
400	Wrong Format (Basic)
401	Wrong Format (Transaction Specific)
402	(GP) Wrong Format or Parameter(s) Missing
500	Transaction Type not Supported
900	Security ERROR - Please call Support

PaymentTrust Result Codes

ST – Streamline
BMS – Barclays
LY – Lloyds
PH – PaymentTech
PT – PaymentTrust
EC – EuroConnex
PN – Pacnet
NT – Neteller
P2 – Pay2
FS – Swedish Acquirer
BV – Bank of Valleta
FX – Foreign Exchange
3D – 3D Secure Verification/Authentication
NA – Not applicable to any Acquirer

Message Code	Description	Explanation	Acquirer
--------------	-------------	-------------	----------

Message Code	Description	Explanation	Acquirer
2000	No answer	Received no answer from banking network. Resend transaction.	PH
2001	Dropped the transaction	No need to do this transaction	NA
2040	Pending to be finalized	Request submitted and waiting for processing to be completed next cycle.	ALL
2050	Request pending	Request submitted and waiting for processing to be completed next cycle.	ALL
2051	Request Pending with Errors.	Cannot find the BTID for the original request	PN
2053	Notification Received	Notification Received	PN
2100	Transaction Authorized/Approved	Transaction Authorized/Approved	ALL
2101	Validated	Validated	NA
2102	Verified	Verified	NA
2103	Prenoted	Prenoted	NA
2104	Transaction approved	Transaction was approved - Base 24	NA
2105	Notification Cleared	Notification Cleared	PN
2150	Funds deposited successfully	Deposit request previously submitted has been processed successfully	NA
2160	Funds refunded successfully	Refund request previously submitted has been processed successfully	NA
2170	Transaction cancelled successfully	Cancellation request has been processed successfully	PT
2200	Transaction Declined	Transaction Declined/Not Authorized/Not Settled	ALL
2202	Cancellation Declined	Cancellation Declined by Acquirer	LY
2203	Cancellation cannot be performed.	Cancellation transaction failed.	PT
2204	Soft AVS	Card was authorized but AVS did not match. Contact client.	PH
2206	Invalid currency	Incoming record currency type does not match system stored currency	PT
2208	Invalid merchant account number	Invalid merchant account number	PT
2210	Invalid credit card number	Bad check digit, length, or other credit card problem	PT
2212	Invalid credit card expiration date	Credit card has expired or incorrect date entered. Confirm date.	PT, EC, LY, PH and BV
2214	Credit card expired	Credit card has expired	AX, FS, LY and PH
2216	Invalid amount	Amount sent was 0 or unreadable	PT
2218	Invalid method of payment	Method of payment is invalid for this account number	PT
2219	Credit card is not valid for this transaction	The specific credit card will not accept payment.	BACS
2220	Invalid method of payment for merchant account number	Method of payment is invalid for this merchant	PT
2222	Invalid field data	Invalid information entered	LY and PH
2223	No Sort code or Account Number in Payback system	No Sort code or Account Number in Payback system	BACS

Message Code	Description	Explanation	Acquirer
2224	Data is inaccurate or missing	Specific and relevant data within transaction is inaccurate or missing	PT
2226	Duplicated transaction	Same transaction had been submitted	FS, PH and BV
2228	Invalid transaction	Issuer does not allow this transaction	PT
2229	Invalid transaction	Processor permits only one deposit request per authorization	PT
2230	Invalid merchant account number	Invalid merchant account number	AX
2232	Invalid issuer	Invalid issuer or institution	FS
2234	Invalid response code	Invalid response code	PH
2235	Invalid Currency Code Entered	Currency code submitted is different than code submitted with original authorization request	PH
2236	Invalid for credit	Invalid for credit	PH
2237	Invalid refund not allowed (CFT)	Invalid refund not allowed (CFT)	LY, BC, ST, FS
2238	Invalid for debit	Invalid for debit	PH
2240	Invalid SEC code - Amex	Amex CID is incorrect	PH
2280	Incorrect start date	Switch/Solo - Incorrect start date or requires an issue number. Please correct	PH, BMS, ST and LY
2282	Invalid issue number	Switch/Solo - 1-digit number submitted when 2-digit number should have been sent. Please correct	PH, BMS, ST and LY
2284	Invalid transaction	Switch/Solo - a format issue, re-examine transaction layout. Please correct	PH, BMS, ST and LY
2286	Bank not supported by Switch	Bank not supported by Switch	PH
2300	Card does not exist	No card record	NA
2302	Invalid transit routing number (ABA code)	Invalid bank routing number	PH
2304	Missing name	Missing the check writer's name.	PH
2306	Bank account closed	Bank account has been closed	PH
2308	Invalid account type	Account type is invalid or missing. Deposit transactions only	PH
2310	Account does not exist	Account does not exist	PH
2312	No account	Account number does not correspond to the individual	PH
2314	Account holder deceased	Account holder deceased. No further debits will be accepted by the bank	PN
2316	Beneficiary deceased	Beneficiary deceased. No further debits will be accepted by the bank	NA
2318	Account frozen	The funds in this account are unavailable. No further debits will be accepted by the bank	NA
2320	Customer opt out	Customer has refused to allow the transaction	NA
2322	ACH non-participant	Banking institute does not accept ACH transactions (For US ECP)	PH
2324	Invalid account number	Account number is incorrect	FS, LY, NT, P2 and PH
2326	Authorization revoked by customer	Customer has notified their bank not to accept these transactions	PH

Message Code	Description	Explanation	Acquirer
2328	Customer advises not authorized	Customer has not authorized bank to accept these transactions	PH
2330	Invalid CECP action code	Pertains to Canadian ECP only.	PH
2332	Invalid account number format	Format of account number does not pass check digit routine for that institution. (For CDN ECP)	PH
2334	Bad account number data	Invalid characters in account number	PH
2350	Card surpassed daily limit	Card has surpassed daily transaction amount limit	PH
2352	Times card used limit	The limit of number of times used for the card has been surpassed	PH
2354	Over credit limit	Card has surpassed its credit limit	LY and PH
2356	Enter lesser amount	Enter a lesser amount	NA
2358	No credit amount	No credit amount	NA
2360	One purchase limit	Card is limited to one purchase	PH
2362	Over Sav limit	Over Sav limit	BV
2364	Over Sav frequency.	Over Sav frequency.	PH
2366	Card not supported	Card not supported	LY
2368	Invalid PIN.	Invalid PIN	EC, FS and PH
2370	Allowable PIN tries exceeded.	Allowable PIN tries exceeded	PH and BV
2372	PIN required	PIN required	BV
2374	Card failed MOD 10 check	Card failed MOD 10 check verification	BV
2380	On negative file	Account number appears on negative file	LY, PH and BV
2382	Stop Payment Issued	Stop Payment Issued	PN
2400	PTLF full	PTLF full	BV
2401	Fraud suspected	Fraud suspected	NA
2402	Unable to process transaction	Unable to process transaction	NA
2403	Duplicate transaction	Duplicate transaction	LY
2404	Cutoff in progress	Cutoff in progress	PN
2405	Incorrect PIN	Incorrect PIN	FS, LY, NT and BV
2406	PIN tries exceeded	PIN tries exceeded	FS and LY
2407	Exceeds withdrawal frequency	Exceeds withdrawal frequency	FS and LY
2410	Invalid 3D Secure Data	Invalid 3D Secure Data	BMS, ST and LY
2610	Timeout error	Timeout waiting for host response	FS, AX, BV, ST and LY
2611	Timeout error	Internal timeout	PT
2612	Authorization host system down or unavailable	Authorization host system is temporarily unavailable	ST, PH and BV
2614	Acquirer/Issuer unavailable. Resend	Authorization host network could not reach the bank, which issued the card or Acquirer.	BMS. ST, LY, EC, AX and PH
2616	Invalid issuer	Invalid issuer or institution	LY and PH

Message Code	Description	Explanation	Acquirer
2618	Unidentified error	Unidentified error. Unable to process transaction	BMS, ST, PH and BV
2620	Unable to process.	Unable to process transaction due to system malfunction	FS, LY and BV
2622	Unable to authorize.	Unable to authorize due to system malfunction	LY and BV
2624	Merchant information incomplete	Merchant information incomplete	NT and P2
2626	Invalid CVN value	Invalid CVN value	FS and LY
2627	Invalid track2 data	The track2 format information is incorrect	PT
2628	Transaction not supported	Merchant not Support this transaction	LY
2630	Invalid store ID	No such store ID for the merchant	PT
2632	Invalid authcode	Invalid authcode	NA
2634	Invalid format	Invalid format	AX and LY
2636	Invalid message type	Invalid message type	NA
2638	Invalid POS system type	Invalid POS system type	NA
2640	This transaction has been cancelled	A message has be sent to reverse previous time out transaction	AX and LY
2642	This TrxSource is not supported by the bank	This TrxSource is not supported by the bank	PT
2644	Insufficient Terminal IDs, please try again	Not enough terminal ID at the time of transaction	ST
2700	Invalid file	General error for PC card	NA
2702	Amounts do not compute	Amount is invalid	PT
2704	Line items do not add up to summary total	Line items do not add up to summary total	PT
2706	Not supported for batch	Not supported for batch	PT
2712	Mandatory field is invalid or missing	Mandatory field is invalid or missing	PT
2714	Total line items do not add up	Total line items do not add up	PT
2716	Line items missing	Line items missing	NA
2718	Commodity code is invalid or missing	Commodity code is invalid or missing	AX
2720	Cross border information is invalid or missing	Cross border information is invalid or missing	PT
2722	Invalid purchase card number	Not a purchase card	PT
2802	Invalid ICC parameter.	One of the ICC parameters submitted was invalid.	PT
2952	Pick up card	Card issuer wants card returned. Call issuer	EC, LY, PH and BV
2954	Card stolen	Card reported as lost/stolen	FS, LY, PH and BV
2956	Do not honour	Generic decline. No other information is being provided by the issuer	FS, LY and PH
2958	Call Bank	Issuer wants voice contact with cardholder	AX, ST, BMS, EC, FS, LY, BV and PH
2960	Insufficient funds	Insufficient funds	FS, LY, NT, P2 and PH
2962	CVV2 failure	Issuer has declined request because CVV2 edit failed	LY and PH

Message Code	Description	Explanation	Acquirer
2964	Delinquent account.	Delinquent account	BV
2990	Cancellation	Cancellation is going to reverse the authorization	NA
3050	Transaction pending	Transaction pending	FX
3051	Transaction pending with rate escalated	A new rate is assigned for the transaction	FX
3100	Transaction approved	FX transaction approved	FX
3111	Rate escalated	Transaction rate escalated	FX
3170	Transaction cancelled successfully	Transaction cancelled successfully	FX
3171	Transaction refunded	Transaction refunded	FX
3200	Rate expired	Rate requested has expired and no new rate is available	FX
3203	Cancellation cannot be performed	The deposit/refund transaction being cancelled cannot be because it has already been submitted	FX
3204	Cancellation not enabled	Cancellation disabled in merchant set-up	FX
3206	Invalid currency	Invalid currency of record	FX
3207	Exchange currency not supported	Exchange currency not setup in merchant account	FX
3208	CurrencyId matches ConvertedCurrencyId	Conversion to same currency redundant	FX
3209	Currency pair not supported	Cannot convert to requested currency	FX
3210	CurrencyId does not match FX request	Currency submitted does not match the original rate request	FX
3216	Invalid amount	Invalid amount	FX
3217	Invalid FXID	Invalid FXID	FX
3218	Issuer is not available. Please try again	Unexpected error	FX
3219	Credit card is not valid for this transaction	Credit card is not valid for this transaction	FX
3220	Currency Not Supported	Currency of card not supported	FX
3224	Data is inaccurate or missing	One or more required parameters are not present	FX
3226	Duplicated transaction	Duplicated transaction	FX
3228	Invalid transaction	Generic error message for invalid transactions	FX
3321	Invalid account data	Invalid account data	FX
3341	Non-executable rate	Quoted rate is not executable	FX
3354	Refund amount over limit	Refund is over the original value of the deal	FX
3361	Rate quote invalid	Quoted rate is invalid	FX
3362	Rate expired not escalated	Expired rate cannot be escalated	FX
3371	Rate revoked	Rate has been revoked	FX
3381	Transaction exceeds amount limit	Transaction min/max limits reached	FX
3391	Batch size exceeds the maximum allowed	Batch size exceeds the Maximum allowable size transaction/payment not written to database	FX
3614	FX system unavailable	FX system cannot be reached	FX
3781	Refund not enabled	Refund disabled in merchant set-up	FX
3783	Refund not possible	Refund cannot be processed	FX
3785	Refund period expired	Refund period expired	FX
4050	Cardholder enrolled	Cardholder enrolled for 3D Secure	3D
4100	Cardholder authenticated	Cardholder answered password/challenge question correctly	3D
4200	Cardholder not enrolled	Cardholder not enrolled for 3D Secure	3D

Message Code	Description	Explanation	Acquirer
4202	Card not participating in 3D Secure	Credit card is not recognized as a 3D Secure card	3D
4204	Cardholder not authenticated	Cardholder failed to answer password/challenge question	3D
4206	Invalid currency	Invalid currency	3D
4207	Invalid merchant setup. Please call support.	Invalid merchant setup. Please call support.	3D
4208	Invalid merchant account number	Invalid merchant account number	3D
4210	Invalid credit card number	Invalid credit card number	3D
4212	Invalid credit card expiration date	Invalid credit card expiration date	3D
4216	Invalid amount	Invalid amount	3D
4224	Data is inaccurate or missing	Specific and relevant data within transaction is inaccurate or missing	3D
4228	Invalid transaction	Invalid transaction	3D
4240	Cardholder enrolment failed	Enrolment process failed	3D
4242	Cardholder authentication failed	Authentication process failed	3D
4614	MPI not available	MPI not available	3D
4616	Directory server not available	Directory server not available	3D
4618	Internal MPI error	Internal MPI error	3D
4626	Invalid SecureId	Invalid SecureId	3D

13. APPENDIX VI: CURRENCY CODES

The ability to accept new currencies will enable you to attract a larger customer base. Processing in multiple currencies eliminates your customers' foreign exchange risks and issues, which typically stem from local charges to foreign credit cards. PaymentTrust™ currently processes Visa®, Master Card®, and American Express® transactions in the following currencies:

Country Name	Country Code	Currency Name	Currency ID	Currency Code
AUSTRALIA	AUS	AUSTRALIAN DOLLAR	36	AUD
AUSTRIA	AUT	SCHILLING	40	ATS
BAHRAIN	BHR	BAHRAINI DINAR	48	BHD
BELGIUM	BEL	BELGIAN FRANC	56	BEF
BERMUDA	BMU	BERMUDIAN DOLLAR	60	BMD
BRAZIL	BRA	BRAZILIAN REAL	986	BRL
CANADA	CAN	CANADIAN DOLLAR	124	CAD
COLOMBIA	COL	COLOMBIAN PESO	170	COP
CYPRUS	CYP	CYPRUS POUND	196	CYP
CZECH REPUBLIC	CZE	CZECH KORUNA	203	CZK
DENMARK	DNK	DANISH KRONE	208	DKK
EUROPEAN UNION	EUR	EURO	978	EUR
FINLAND	FIN	MARKKA	246	FIM
FRANCE	FRA	FRENCH FRANC	250	FRF
FRENCH POLYNESIA	PYF	CFP FRANC	953	XPF
GERMANY	DEU	DEUTSCHE MARK	280	DEM
GREECE	GRC	DRACHMA	300	GRD
HONG KONG	HKG	HONG KONG DOLLAR	344	HKD
HUNGARY	HUN	FORINT	348	HUF
ICELAND	ISL	ICELAND KRONA	352	ISK
INDIA	IND	INDIAN RUPEE	356	INR
INDONESIA	IDN	INDONESIAN RUPIAH	360	IDR
IRELAND	IRL	IRISH POUND	372	IEP
ISRAEL	ISR	SHEKEL	376	ILS
ITALY	ITA	ITALIAN LIRA	380	ITL
JAMAICA	JAM	JAMAICAN DOLLAR	388	JMD
JAPAN	JPN	YEN	392	JPY
JORDAN	JOR	JORDANIAN DOLLAR	400	JOD
KOREA, REPUBLIC OF	KOR	WON	410	KRW
KUWAIT	KWT	KUWAITI DINAR	414	KWD
LUXEMBOURG	LUX	LUXEMBOURG FRANC	442	LUF
MALAYSIA	MYS	MALAYSIAN RINGGIT	458	MYR
MALTA	MLT	MALTESE LIRA	470	MTL
MEXICO	MEX	MEXICAN NUEVO PESO	484	MXN
MOROCCO	MAR	MOROCCAN DIRHAM	504	MAD
NETHERLANDS	NLD	NETHERLANDS GUILDER	528	NLG
NEW ZEALAND	NZL	NEW ZEALAND DOLLAR	554	NZD
NORWAY	NOR	NORWEGIAN KRONE	578	NOK
OMAN	OMN	RIAL OMANI	512	OMR
PANAMA	PAN	BALBOA	590	PAB
PHILIPPINES	PHL	PHILIPPINE PESO	608	PHP
POLAND	POL	NEW ZLOTY	985	PLN
PORTUGAL	PRT	PORTUGUESE ESCUDO	620	PTE
QATAR	QAT	QATARI RIAL	634	QAR
RUSSIAN FEDERATION	RUS	RUSSIAN RUBLE	643	RUB
SAUDI ARABIA	SAU	SAUDI RIYAL	682	SAR
SINGAPORE	SGP	SINGAPORE DOLLAR	702	SGD
SOUTH AFRICA	ZAF	RAND	710	ZAR

Country Name	Country Code	Currency Name	Currency ID	Currency Code
SPAIN	ESP	SPANISH PESETA	724	ESP
SWEDEN	SWE	SWEDISH KRONA	752	SEK
SWITZERLAND	CHE	SWISS FRANC	756	CHF
TAIWAN	TWD	NEW TAIWAN DOLLAR	901	TWD
THAILAND	THA	BAHT	764	THB
TURKEY	TUR	TURKISH LIRA	792	TRL
TURKEY	TUR	NEW TURKISH LIRA	949	TRY
UNITED ARAB EMIRATES (UAE)	ARE	UAE DIRHAM	784	AED
UNITED KINGDOM	GBR	POUND STERLING	826	GBP
UNITED STATES OF AMERICA	USA	US DOLLAR	840	USD
UZBEKISTAN	UZS	UZBEKISTAN SUM	860	UZS
VENEZUELA	VEN	BOLIVAR	862	VEB

14. APPENDIX VII: COUNTRY CODES

Country Name	ISO Country Code
Afghanistan	AF
Albania	AL
Algeria	DZ
American Samoa	AS
Andorra	AD
Angola	AO
Anguilla	AI
Antarctica	AQ
Antigua and Barbuda	AG
Argentina	AR
Armenia	AM
Aruba	AW
Australia	AU
Austria	AT
Azerbaijan	AZ
Bahamas	BS
Bahrain	BH
Bangladesh	BD
Barbados	BB
Belarus	BY
Belgium	BE
Belize	BZ
Benin	BJ
Bermuda	BM
Bhutan	BT
Bolivia	BO
Bosnia and Herzegovina	BA
Botswana	BW
Bouvet Island	BV
Brazil	BR
British Indian Ocean Territory	IO
Brunei Darussalam	BN
Bulgaria	BG
Burkina Faso	BF
Burundi	BI
Cambodia	KH
Cameroon	CM
Canada	CA

Country Name	ISO Country Code
Cape Verde	CV
Cayman Islands	KY
Central African Republic	CF
Chad	TD
Chile	CL
China	CN
Christmas Island (Australia)	CX
Cocos (Keeling) Islands	CC
Colombia	CO
Comoros	KM
Congo	CG
Cook Islands	CK
Costa Rica	CR
Cote D'Ivoire (Ivory Coast)	CI
Croatia (Hrvatska)	HR
Cuba	CU
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Djibouti	DJ
Dominica	DM
Dominican Republic	DO
East Timor	TP
Ecuador	EC
Egypt	EG
El Salvador	SV
Equatorial Guinea	GQ
Eritrea	ER
Estonia	EE
Ethiopia	ET
Faeroe Islands	FO
Falkland Islands (Malvinas)	FK
Fiji	FJ
Finland	FI
France	FR
French Guiana	GF
French Polynesia	PF
Gabon	GA
Gambia	GM
Georgia	GE
Germany	DE
Ghana	GH
Gibraltar	GI

Country Name	ISO Country Code
Great Britain	GB
Greece	GR
Greenland	GL
Grenada	GD
Guadeloupe	GP
Guam	GU
Guatemala	GT
Guinea	GN
Guinea Bissau	GW
Guyana	GY
Haiti	HT
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Iran	IR
Iraq	IQ
Ireland	IE
Isle of Man (U.K.)	IM
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Johnston Island	JT
Jordan	JO
Kazakhstan	KZ
Kenya	KE
Kiribati	KI
Korea (North)	KP
Korea (South)	KR
Kuwait	KW
Kyrgyzstan	KG
Lao P.Dem.R.	LA
Latvia	LV
Lebanon	LB
Lesotho	LS
Liberia	LR
Libyan Arab Jamahiriya	LY
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU

Country Name	ISO Country Code
Macau	MO
Macedonia	MK
Madagascar	MG
Malawi	MW
Malaysia	MY
Maldives	MV
Mali	ML
Malta	MT
Marshall Islands	MH
Martinique	MQ
Mauritania	MR
Mauritius	MU
Mexico	MX
Micronesia	FM
Midway Islands	MI
Moldova	MD
Monaco	MC
Mongolia	MN
Montserrat	MS
Morocco	MA
Mozambique	MZ
Myanmar	MM
Namibia	NA
Nauru	NR
Nepal	NP
Netherlands	NL
Netherlands Antilles	AN
New Caledonia	NC
New Zealand	NZ
Nicaragua	NI
Niger	NE
Nigeria	NG
Niue	NU
Norfolk Island	NF
Northern Mariana Islands	MP
Norway	NO
Oman	OM
Pakistan	PK
Palau	PW
Panama	PA
Papua New Guinea	PG
Paraguay	PY
Peru	PE

Country Name	ISO Country Code
Philippines	PH
Pitcairn	PN
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Reunion	RE
Romania	RO
Russian Federation	RU
Rwanda	RW
Saint Helena	SH
Saint Kitts and Nevis	KN
Saint Lucia	LC
Saint Pierre and Miquelon	PM
Saint Vincent and The Grenadines	VC
Samoa	WS
San Marino	SM
Sao Tome and Principe	ST
Saudi Arabia	SA
Senegal	SN
Seychelles	SC
Sierra Leone	SL
Singapore	SG
Slovakia	SK
Slovenia	SI
Solomon Islands	SB
Somalia	SO
South Africa	ZA
Spain	ES
Sri Lanka	LK
Sudan	SD
Suriname	SR
Svalbard and Jan Mayen Islands	SJ
Swaziland	SZ
Sweden	SE
Switzerland	CH
Syrian Arab Rep.	SY
Taiwan	TW
Tajikistan	TJ
Tanzania	TZ
Thailand	TH
Togo	TG
Tokelau	TK

Country Name	ISO Country Code
Tonga	TO
Trinidad and Tobago	TT
Tunisia	TN
Turkey	TR
Turkmenistan	TM
Turks and Caicos Islands	TC
Tuvalu	TV
Uganda	UG
Ukraine	UA
United Arab Emirates	AE
United States	US
Uruguay	UY
Uzbekistan	UZ
Vanuatu	VU
Vatican City State (Holy See)	VA
Venezuela	VE
Viet Nam	VN
Virgin Islands (British)	VG
Virgin Islands (US)	VI
Wake Island	WK
Wallis and Futuna Islands	WF
Western Sahara	EH
Yemen	YE
Yugoslavia	YU
Zaire	ZR
Zambia	ZM
Zimbabwe	ZW

15. APPENDIX VIII: STATE/PROVINCE/REGION CODES

State/Region	Code	Country
Alabama	AL	us
Alaska	AK	us
American Samoa	AS	us
Arizona	AZ	us
Arkansas	AR	us
Armed Forces - Europe	AE	us
Armed Forces - Pacific	AP	us
Armed Forces - The Americas	AA	us
California	CA	us
Colorado	CO	us
Connecticut	CT	us
Delaware	DE	us
District of Columbia	DC	us
Federated States of Micronesia	FM	us
Florida	FL	us
Georgia	GA	us
Guam	GU	us
Hawaii	HI	us
Idaho	ID	us
Illinois	IL	us
Indiana	IN	us
Iowa	IA	us
Kansas	KS	us
Kentucky	KY	us
Louisiana	LA	us
Maine	ME	us
Marshall Islands	MH	us
Maryland	MD	us
Massachusetts	MA	us
Michigan	MI	us
Minnesota	MN	us
Mississippi	MS	us
Missouri	MO	us
Montana	MT	us
Nebraska	NE	us
Nevada	NV	us
New Hampshire	NH	us
New Jersey	NJ	us

State/Region	Code	Country
New Mexico	NM	us
New York	NY	us
North Carolina	NC	us
North Dakota	ND	us
Northern Mariana Islands	MP	us
Ohio	OH	us
Oklahoma	OK	us
Oregon	OR	us
Palau	PW	us
Pennsylvania	PA	us
Puerto Rico	PR	us
Rhode Island	RI	us
South Carolina	SC	us
South Dakota	SD	us
Tennessee	TN	us
Texas	TX	us
Utah	UT	us
Vermont	VT	us
Virgin Islands	VI	us
Virginia	VA	us
Washington	WA	us
West Virginia	WV	us
Wisconsin	WI	us
Wyoming	WY	us
Alberta	AB	ca
British Columbia	BC	ca
Manitoba	MB	ca
New Brunswick	NB	ca
Newfoundland	NF	ca
Nova Scotia	NS	ca
Northwest Territories	NT	ca
Nunavut	NN	ca
Ontario	ON	ca
Prince Edward Island	PE	ca
Quebec	QC	ca
Saskatchewan	SK	ca
Yukon	YT	ca
Eastern Cape	EC	za
Free State	FS	za
Gauteng	GG	za
KwaZulu-Natal	KN	za
Mpumalanga	MG	za
Northern Cape	NO	za

State/Region	Code	Country
Northern Province	NP	za
North West	NW	za
Western Cape	WC	za
Australian Capital Territory	ACT	au
New South Wales	NSW	au
Northern Territory	NT	au
Queensland	QLD	au
South Australia	SA	au
Tasmania	TAS	au
Victoria	VIC	au
Western Australia	WA	au

16. APPENDIX IX: HOW TO CONTACT US

Our product support specialists provide technical assistance to current customers or maintenance customers, prospective customers who are evaluating our products and services. Our support specialists handle questions on the use, configuration and functionality of our products and services and are committed to providing timely responses to your enquiries.

Contact us at support@paymenttrust.com.

Supportline (office hours)

Dialing from within the UK - 0845 3007567

Dialing from outside the UK - +44 (0) 1932 690237

17. GLOSSARY OF PAYMENT PROCESSING TERMINOLOGY

A

ABA

See American Bankers Association.

ABA Routing Number

The American Bankers Association (ABA) routing number is a unique, bank identifying number that directs electronic ACH deposits to the proper bank. The routing number precedes the account number printed at the bottom of a check and is usually printed with magnetic ink.

Account Number

A unique sequence of numbers assigned to a cardholder's account, which identifies the issuer and type of financial transaction card.

ACH

See Automated Clearing House.

ACI

See Authorization Characteristics Indicator.

Acquirer

A bank or financial institution that acquires data relating to transactions from a merchant or card acceptor for processing. The acquirer enters this data into interchange, either directly or indirectly. See Interchange.

Acquiring Bank

A bank that receives credit card transactions and then deposits them with the issuing banks. This is an acquirer.

Address Verification Service

A service that verifies the cardholder's billing address in order to help combat fraud in card-not-present transactions (e.g. mail order, telephone order, internet, etc.). Used only in the United States.

Agent Bank

A bank that participates in another bank's acquiring program, usually by turning over its applicants for bank cards to the bank administering the acquiring program.

American Banker's Association

The trade association of American bankers. This body also has the responsibility of assigning the registration authority for identification numbers.

American Express

An organization that issues cards and acquires transactions, unlike Visa and MasterCard, which are bank associations. American Express processes their own transactions through their network.

Amex

See American Express.

API

The Application Programming Interface (API) is the interface by which an application program

accesses the operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel to ensure the portability of the code.

Approval

Any transaction that is approved by the cardholder or the check issuer's bank. Approvals are requested via an authorization. An approval is the opposite of a declined transaction.

Arbitration

The procedure used to determine the responsibility for a chargeback-related dispute between a merchant and buyer.

Asynchronous

A method of transmitting data in which the data elements are identified with special start and stop characters. An asynchronous modem cannot communicate with a synchronous modem. Compare with *Synchronous* (e.g. standard Hayes compatible modem).

ATM

See Automated Teller Machine.

Auth Only

A transaction in which the merchant does not intend to charge the cardholder until a later time, if at all. See Prior Authorized Sale.

Authorization

An authorization is a request to charge a cardholder. It reduces the cardholder's open to buy, but does not actually capture the funds. An authorization is the first transaction in the delayed deposit process. It does not bill the card until a delayed capture transaction is issued. The authorization must be deposited in order to charge the account. If it is not used within a certain time period, it will drop off. The issuing bank determines the time period for drop off. Authorizations can only be used for credit card transactions.

Authorization Code

Approved sale and authorization transactions always receive a numeric or alphanumeric authorization code referencing the transaction for processing purposes.

Automated Clearing House

The Automated Clearing House (ACH) network is a nationwide, wholesale electronic payment and collection system. It is a method of transferring funds between banks via the Federal Reserve System. Most, but not all, financial institutions use it.

Average Ticket

The average dollar amount of merchant credit transactions.

AVS

See Address Verification Service.

B**Bank card**

A debit or credit card issued by a bank.

Bank Identification Number

The digits of a credit card that identifies the issuing bank. It is sometimes the first six digits and is often referred to as a BIN. Also referred to as Issuer Identification Number.

Basis Point

One one-hundredth of a percent. Discount rates are expressed as basis points.

Batch

A collection of transactions submitted for deposit. Usually a merchant has one batch per day or per shift.

Batch ID

Once a batch is deposited, it is assigned a batch ID. Every transaction in the batch shares this ID. If a transaction does not have a batch ID associated with it, the transaction has not been deposited.

Batch Processing

A type of data processing where related transactions are transmitted as a group for processing.

Batch Deposit

An electronic bookkeeping procedure that sends all funds from captured transactions to the merchant's acquiring bank for deposit. PaymentTrust™ automatically submits all captured transactions for deposit on a daily basis. The time span, in which funds reach the merchant account after deposit, is 1-5 days, but varies by acquiring bank.

BIN

See Bank Identification Number.

Binary Executable

A universal character coding system.

Bundled Rate

A discount rate that includes communication costs as well as transaction fees. Also referred to as a flat rate.

C**Cancellation**

Reversal of a partial or an entire authorization charge prior to the deposit process. It prevents a transaction from being deposited. A Cancellation does not remove any hold on the cardholder's open to buy.

Capture

The process of capturing funds from an authorized transaction.

Card Issuer

See Issuer, Issuing Bank.

Card-Not-Present

A merchant environment where the cardholder and the card are not physically present at the time of purchase. The following are typical card-not-present transactions: mail/telephone order, business to business and internet based transactions.

Card-Present

A merchant environment where the cardholder and the card are physically present at the time of purchase. Card-present transactions account for the majority of credit card transactions in the world.

Card Verification Value

A unique verification value encoded on the magnetic strip of a card to validate card information during the authorization process. The card verification value is calculated from the data encoded on the magnetic strip using a secure cryptographic process. This method is used by Visa and Master Card.

CAV

Cardholder Authentication Value used by PaymentTrust Ltd. and Acquirer. Base64 encoded data structure containing 3D Secure authentication results provided by the 3D Secure MPI, usually Visa's CAVV or MasterCard's UCAF.

CAVV

Visa's Cardholder Authentication Verification Value. Base64 encoded data structure containing 3D Secure authentication results provided by the 3D Secure MPI.

CGI

See Common Gateway Interface.

Chargeback

The act of taking back funds that have been paid to a merchant for a disputed or improper credit card transaction. The issuer can initiate this procedure 30 days after the deposit.

Chargeback Period

The number of calendar days in which a card member may charge sales back to the merchant, beginning with the day after the date the record is first received by the member or agent and continuing until the end of the day on which it is dispatched as a chargeback item.

Chargeback Reason Code

A two-digit code identifying the specific reason for the chargeback.

Check Guarantee

A service which guarantees check payments (up to the limit defined for the account) provided that the merchant follows correct procedures in accepting the check. The service determines whether the check issuer has previously written delinquent checks. Companies like TeleCheck provide this type of service.

Chip Card

Also known as a smart card. A chip card holds details on a computer chip, which can store and process information. It usually also has a traditional magnetic stripe.

Clearing

The process of exchanging financial details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a merchant's deposit position.

Common Gateway Interface

An interface program that enables an Internet server to run external programs to perform a specific function. Also referred to as gateways or CGI scripts; these programs generally consist of a set of instructions written in a programming language like C or PERL that process requests from a browser, executes a program and formats the results in HTML. Gateway scripts often add interactivity to a Web page by enabling users to fill out and submit forms for processing.

Confirmation Letter

A letter sent by a processor to a merchant on a daily or weekly basis to verify batch deposits.

Converted Currency ID

ISO standard numeric ids of the converted currency.

Example: USA = 840, GBP = 826, JPY = 392

Conversion Rate

The conversion rate applied to the transaction amount in U.S. dollars.

Copy Request

See Retrieval Request.

Credit

Also known as a refund. A credit is a transaction that transfers funds from the merchant's account back in to the customer's credit card. This type of transaction is usually performed when a product is returned to the merchant. A credit can be performed through the e-Transaction Terminal area of PaymentTrust™ Payment Manager or through a merchant's storefront application. Check refunds can only be issued via credit card or through a non-electronic paper check. A credit can only be issued to an account that has not had a previous authorization.

Credit Limit

The limit of credit a cardholder is approved to borrow. Credit card purchases are loans to the cardholder by the issuer.

Currency ID

ISO standard numeric ids of the converted currency.

Example: USA = 840, GBP = 826, JPY = 392

CVC

See Card Verification Code.

CVV

See Card Verification Value.

CVV2

See Card Verification Value.

D**DDA**

See Demand Deposit Account.

Debit Card

An ATM bank card used to purchase goods and services, and to obtain cash. A debit card debits the cardholder's bank account and requires a Personal Identification Number (PIN). Debit cards branded with a bank card logo (e.g. Visa) can be accepted without a PIN for Internet transactions.

Decline

A transaction in which the issuing bank will not authorize the transaction.

Delayed Capture

A delayed capture is a transaction type that uses the information from an authorization transaction to capture funds. This is the second step in the delayed deposit process and should be used by merchants who do not provide immediate shipment of goods.

Delayed Deposit

This is a two-phase process that utilizes an authorization and a delayed capture transaction to process customer orders. This procedure is recommended when the merchant delivers goods or services after a 48-hour period.

Demand Deposit Account

A standard checking or savings account into which electronic funds can be transferred.

Deposit

The process of transmitting a batch of transactions from the merchant to the acquiring institution for deposit preparation. It marks a previously authorized transaction for funds capture during the next deposit period. Merchants who do not ship goods immediately should use this transaction type after fulfilling their sales obligation.

Discount fee

Fee paid by the merchant to the merchant bank or other contracted party for processing the merchant's credit card sales transactions.

Discount Rate

Amount charged to a merchant by the acquiring bank for transaction processing. It usually represents a percentage of the transaction amount. The rate is typically based on monthly transaction volume (total dollars) and average ticket. The discount fee is the dollar amount charged.

Downgraded ICC:

A chip card that only contains track 2 information on it.

Draft Capture

Refers to Deposit.

E**ECR**

See Electronic Cash Register.

EFT

See Electronic Funds Transfer.

Electronic Cash Register

The combination of a cash register and a POS terminal, often PC based.

Electronic Funds Transfer

The paperless act of transmitting money through a computer network.

External Sales Agent

Amex term for ISO or MSP.

F**Floor Limit**

A preset limit established by an issuer that allowed merchants to accept credit card sales without authorization provided the merchant verifies the card number on a warning bulletin for lost or stolen cards. Floor limits are now rarely used.

Fraudulent User

An individual who is not the cardholder or designee and who uses a card to obtain goods or services without the cardholder's consent.

Fraudulent Transaction

A transaction unauthorized by the cardholder of a bank card. Such transactions are categorized as lost, stolen, not received, issued on a fraudulent application, counterfeit, fraudulent processing of transactions, account takeover, or other fraudulent conditions as defined by the card company or the member company.

H**HTTP Protocol**

Hardware and/or software that connects computer networks and allows them to communicate.

I**ICC (Integrated Circuit Card)**

See chip card.

Independent Sales Organization

Visa term for a company that is sponsored by an acquiring bank to solicit and sometimes support merchants.

Interchange

The flow of information between issuers and acquirers (e.g. transactions, retrieval requests, chargebacks).

Interchange Fee

The fee charged by Visa and MasterCard for each credit card transaction. This fee is part of the discount rate.

Internet Merchant Bank Account

A special account required for merchants who wish to sell goods and services over the Internet and accept credit cards as payment. This type of account is different than a typical merchant account and is considered similar to a card-not-present transaction.

Internet Service Provider

A company that offers access to individuals or companies to connect to the Internet.

ISO

See Independent Sales Organization.

ISP

See Internet Service Provider.

Issuer

An institution that issues plastic cards to cardholders.

Issuing Bank

See Issuer.

M**Magnetic Ink Character Recognition (MICR)**

The process used to read the string of numbers on the bottom of a check. The MICR characters (0-9 and 4 special characters) are printed in special toner or ink. When the check is passed

through a reader/sorter, it passes through two magnetic heads. The first one magnetizes the MICR character and the second one reads the (now) magnetic MICR character. Also referred to as Magnetic Ink Check Reader.

Manual Entry

Credit card information that is entered via the e-Transaction Terminal of PaymentTrust™ Payment Manager.

Manual Refund

A transaction that returns the specified amount to the cardholder's account.

MasterCard

An association of banks that governs the issuing and acquiring of MasterCard credit card transactions and Maestro debit transactions.

Member

A financial institution that is a member of Visa USA and/or MasterCard International. A member is licensed to issue cards to cardholders and/or accept merchant drafts.

Merchant

A retailer, or any other entity (pursuant to a Merchant Agreement), that agrees to accept credit cards, debit cards, or both, when properly presented.

Merchant Agreement

A written agreement between a merchant and a bank (or possibly between a merchant, a bank and ISO) summarizing their respective rights, duties and warranties with respect to acceptance of the bank card and matters related to bank card activity.

Merchant Bank

A bank issuing an agreement to a merchant to accept (acquire) deposits generated by bank card transactions.

Merchant Category Code

A code assigned by an acquirer to a merchant to identify the merchant's principal trade, profession, or line of business. This 4-digit code is also known as the SIC code.

Merchant Discount

Compensation received by a bank from a merchant for processing and accepting credit card risk on the merchant's credit card sales.

Merchant Number

A series or group of digits that uniquely identifies the merchant to the merchant's signing bank for account and billing purposes.

Merit

Refers to the qualification levels for a MasterCard transaction. Merit III is the highest discount, followed by Merit II, Merit I, and then Standard.

MICR Number

See Magnetic Ink Character Recognition.

MO/TO

Mail Order/Telephone Order credit card transactions.

MPI

Merchant Plugin. 3rd party software used by a merchant to authenticate 3D Secure transactions.

MSP

See Member Service Provider.

N**Network**

See Processor. Also used to refer to communication networks like AT&T or CompuServe.

Non-Qualified

A broad term that describes a transaction that did not interchange at the best rate, because it was entered manually, was not deposited in a timely manner, or the data set required for the best interchange was not provided.

O**ODFI**

See Originating Depository Financial Institution.

Open to buy

The amount of credit available at a given time on a cardholder's account.

Operator

A central clearing facility that provides distribution and deposit of ACH transactions. ACH operators clear debits and credits electronically, rather manually. Currently four ACH Operators exist: the Federal Reserve System, which clears approximately 80% of all ACH transactions, Visanet ACH, New York ACH, and American ACH.

Original Draft

The original copy of the forms and signatures used in the transaction. Also referred to as the hard copy.

Originating Depository Financial Institution

A financial institution that initiates and warrants electronic payments through the ACH network on behalf of its customers.

Originator

A company or other business entity that creates entries for introduction into the ACH network. For example, a billing company produces debit entries from customers' financial institution accounts who have authorized direct payment for products and services.

P**PAN**

See Primary Account Number.

PIN

Personal Identification Number used by a cardholder to authenticate card ownership for ATM or debit card transactions. The cardholder enters his/her PIN into a keypad. The PIN is required to complete an ATM/debit card transaction.

Point Of Sale

The place and time at which a transaction occurs. Point of Sale (POS) also refers to the devices or software used to capture transactions.

POS

See Point Of Sale.

Post Authorization

A transaction for which a voice authorization was received. See Prior Authorized Sale.

Post-Auth

See Post Authorization.

Posting

The process of recording debits and credits to a cardholder's account balances.

Pre-Auth

Same as Auth Only.

Prenote

See Pre-Notification.

Pre-Notification

Prior to the initiation of the first ACH entry to an ACH receiver or the ACH receiver's account with an RDFI, an ACH originator may, at its option, deliver or send a pre-notification through an ODFI to its ACH operator for transmittal to the appropriate RDFI. The pre-notification shall provide notice to the RDFI that the originator intends to initiate one or more entries to that receiver's account in accordance to the receiver's authorization.

Primary Account Number (commonly called PAN)

The number that is embossed, encoded, or both on a plastic card that identifies the issuer and the particular cardholder account. The PAN consists of a major industry identifier, issuer identifier, individual account identifier, and check digit.

Prior

See Prior Authorized Sale.

Prior Authorized Sale

A transaction for which authorization was obtained before a transaction takes place, e.g. when a merchant has to call for authorization before services are rendered. The approved authorization request may be held for an extended length of time before a card is present or not.

Prior-Auth

See Prior Authorized Sale.

Private Label Card

A bank card that can be used only in a specific merchant's store. Typically not a bank card.

Processing Date

The date on which the acquiring bank processes the transaction.

Processor

A large data center that processes credit card transactions and deposits funds to merchants. A processor connects to the merchant on behalf of an acquirer via a gateway or POS system to process payments electronically. Processors edit and format messages and switch to bank card networks. They provide files for clearing and deposit, and other value added services.

Q

Qualification

A level at which a transaction interchanges. The level of qualification is dependent on how a credit card number is entered, how quickly a transaction is deposited, the type of industry, and other specific information.

R**RDFI**

See Receiving Depository Financial Institution.

Receipt

A hard copy description of the transaction that occurred at the point of sale. Minimum information contained on a receipt is date, merchant name and location, account number, type of account used (e.g. Visa, MasterCard, Amex, etc.), amount, reference number and/or authorization code, and action code.

Receiver

A consumer, customer, employee, or business who has authorized ACH payments by Direct Deposit or Direct Payment to be applied against a depository account.

Receiving Depository Financial Institution

A financial institution that provides depository account services to customers, employees and businesses, and accepts electronic debits and credits to and from these accounts.

Recurring Transaction

A transaction in which a cardholder has given a merchant permission to periodically charge the cardholder's account.

Refund

A transaction that returns the specified amount to the cardholder's account.

Response Code

A numeric code that indicates whether a transaction was approved or declined. Response codes are used in the PaymentTrust™ system to indicate transaction responses to merchants.

Retrieval

See Retrieval Request.

Retrieval Request

A request to a merchant for documentation concerning a transaction, usually initiated by a cardholder's dispute or suspicious sale/return. A retrieval request can lead to a chargeback.

Return Code

Any of the codes returned by PaymentTrust™ when a transaction is processed.

S**Secure Sockets Layer**

An encryption system that allows merchants to securely process electronic transactions.

Deposit

The process by which transactions with authorization codes are sent to the processor for payment to the merchant. Deposit is a sort of electronic bookkeeping procedure that causes all

funds from captured transactions to be routed to the merchant's acquiring bank for deposit. PaymentTrust™ automatically submits all captured transactions for deposit on a daily basis. The time that it takes for these funds to reach the merchant account after deposit is 1-5 days, but varies according to the merchant's agreement with their respective card processing company. Also referred to as Deposit.

SIC Code

Refers to Standard Industry Classification. These codes are 4-digit numbers used to identify a business type.

Simultaneous Authorization And Deposit

Charges the specified amount against the account, and marks the transaction for immediate funds transfer during the next deposit period.

Smart Card

A credit or debit card embodying a computer chip with memory and interactive capabilities used for identification and to store additional data about the cardholder, cardholder's account, or both. Also called an integrated circuit card or a chip card.

SSL

See Secure Sockets Layer.

Standard

The lowest qualification level at which a Visa or MasterCard transaction may interchange. This occurs when a transaction is deposited several days after the original authorization.

Surcharges

Any additional charges to a merchant's standard processing fee. They are a result of non-qualified transactions of different communication methods.

Suspense

A state in which a batch of transactions is not released to interchange, because of problems noticed by the host computer. Requires human intervention to fix the problem and deposit the batch.

Swiped Card

Credit card information that is transferred directly as a result of swiping or sliding the credit card through a card reader. Swiped cards are used in retail and other card-present situations. The information magnetically encoded in the magnetic strip includes confidential data that helps validate the card.

Synchronous

A method of transmitting data in which the data elements are sent at a specific rate so that start and stop characters are not needed. Used by older modems such as, Amex PIP terminals. See Asynchronous.

T**T & E Card**

See Travel and Entertainment Card.

Tender Type

The type of "money" used when processing a transaction, for example, credit card, check, ACH, Purchase Card, etc.

Third Party Processor

A non-member agent employed by an acquiring bank, which provides authorization, deposit and merchant services to the bank's merchant.

Track 1

Bank discretionary data encoded on a magnetic stripe. Includes credit card account number, cardholder name, and expiry date. This magnetic strip is read-only, and its contents are defined in ISO 7813.

Track 2

Bank discretionary data encoded on a magnetic stripe. Track 2 includes credit card account number and expiry date. This magnetic strip is read-only, and its contents are defined in ISO 7813.

Transaction

The action between a cardholder and a merchant that results in activity on the cardholder's account.

Transaction Fee

A per transaction charge in addition to the percentage discount fees, incurred by merchants who are on scale pricing.

Transaction Date

The date on which a transaction between a cardholder and a merchant, an acquirer, or a carrier, occurs.

Transaction ID

A is a 16-character numeric string that PaymentTrust™ assigns to every transaction that it processes.

Transaction Type

A specific financial detail transaction activity that can be submitted to the clearing system

Travel and Entertainment Card

Credit cards that typically require payment in full each month, (e.g. American Express, Diner's Club, and Carte Blanche).

U**UCAF**

MasterCard's Universal Cardholder Authentication Field. Base64 encoded data structure containing 3D Secure authentication results provided by the 3D Secure MPI.

Undeposited Transactions

PaymentTrust™ automatically deposits deposit transactions on a daily basis. Please note that authorization transactions are not captured until they are completed by a deposit transaction. PaymentTrust™ transaction types that are automatically flagged for capture include simultaneous authorization, deposit, and refund.

V**Visa**

An association of banks that governs the issuing and acquiring of Visa credit card transactions.