



Version 1.1 – June 2005



Contents

01. Introduction.....	3
What do Protx do?	3
What are Card-not-present (CNP) transactions?	3
Do I need to worry about CNP Fraud?	4
02. Risks from CNP Transactions on the Internet	5
03. The Internet Transaction Process	6
Merchant	6
Acquiring Bank	6
Card Issuer	7
Card Schemes	7
Visa/MasterCard Directory.....	7
Payment Service Provider.....	7
Transaction Process Diagram	8
04. Protx Fraud Prevention Tools.....	9
AVS/CV2.....	9
AVS/CV2 Response from Protx	10
AVS/CV2 Rules	11
AVS/CV2 Rules and Manual Checks.....	12
Verified By Visa and SecureCode (3D Secure)	13
The 3 rd Man Fraud Prevention	17
Deferred and Preauth transactions.....	19
05. Manual Checks	21
When should you perform manual checks?	21
Possible Fraud Indicators.	21
What manual checks can you perform?	22
06. Other Fraud Prevention Advice	23
High Value and Overseas Transactions	23
Delivery.....	23
Transaction receipt.....	23
VSP Admin.....	23
07. Additional card scheme requirements	24
Mandatory website content requirements	24
Additional website content requirements	24
Protx Security Statement	24
08. The Chargeback Process.....	25
What is a chargeback?.....	25
What happens?.....	25
09. Top 10 Tips	26
10. Glossary of Common Terms	27



01. Introduction

What do Protx do?

Protx are an Internet Payment Service Provider. We provide the software to enable your website to take secure online credit and debit card payments. In order to take secure online payments, you must have an Internet Merchant Account which is provided by your Merchant bank or Acquiring Bank.

Although Protx provides the software facility to allow you to trade online and to ensure that your customer's details remain secure throughout the transaction process, we cannot guarantee against fraudulent transactions.

Importantly, **Authorisation does not guarantee against chargeback's**. You will need to ensure that you have carried out all the necessary checks to ensure that the transaction is not fraudulent. Protx provides several tools to help you in your fight against fraud. These tools are detailed later in this document.

What are Card-not-present (CNP) transactions?

CNP transactions are transactions where the card and cardholder are not present at the point-of-sale. This applies to the following:

- Internet orders
- Mail order
- Telephone orders
- Fax orders

Because the card and cardholder are not present, you are unable to physically check the card or the identity of the cardholder.

You need to be particularly careful about CNP transactions, because it is much easier for the fraudster to disguise their true identity.

When a CNP transaction is processed, Protx requests authorisation from the card issuer via your acquiring bank. The card issuer will then confirm that card has not been reported lost or stolen, and that the cardholder has sufficient funds on their account.



Do I need to worry about CNP Fraud?

CNP fraud in the UK is growing daily and the rate of growth has increased significantly in the last few years.

In 2002 CNP fraud cost businesses £110.1 million, a 15% increase over 2001 (source APACS).

The internet has opened the international market to UK businesses. With overseas orders come extra risks which can be difficult to tackle and you should pay particular attention to these orders.

You are responsible for ensuring that CNP transactions are not fraudulent. If a transaction is fraudulent, you will be liable for the loss.

You need to ensure that you have procedures in place to protect your business against fraud.





02. Risks from CNP Transactions on the Internet

The internet is currently the fastest growing area for making CNP purchases. Because the internet enables an individual to disguise their identity, it gives them much greater confidence when using card details fraudulently.

Some of the factors which make the Internet a higher risk for CNP transactions include:

- Overseas orders
- No centralised standards or legal authority
- Weak customer identification mechanisms



03. The Internet Transaction Process

Protix and you, as the merchant, are not the only parties involved in the transaction process for Internet CNP transactions. There are actually several parties involved:

Merchant

The vendor or retailer is the party selling goods or services via the Internet. In this case it would be you. If you are new to trading on the Internet you need to obtain permission from your acquiring bank. You are responsible for ensuring that transactions are placed by the genuine cardholder and are therefore liable if the genuine cardholder disputes the transaction.

Acquiring Bank

The acquiring bank provides you with an Internet merchant number to allow you to take credit and debit card transactions online.

The acquiring bank deals with the processing and settlement of funds for each transaction. They will help you to process a chargeback (see page 21 for more information) with the card issuer.

Protix are currently approved with the following acquiring banks:

- Lloyds TSB Cardnet
- Barclaycard Merchant Services
- NatWest Streamline
- HSBC
- Bank of Scotland
- American Express
- Diners Club
- JCB



Card Issuer

The card issuer is the financial institution that provides the cardholder with their credit or debit card. The card issuer is contacted by the acquiring bank during the transaction process. The following details are confirmed:

- The card number exists
- The expiry date is correct (not for all transactions)
- The card has not been reported lost or stolen
- There are sufficient funds in the account at that given moment in time

The card issuer may also check the AVS/CV2 details (see page 9 for details) if this information has been provided in the transaction message. Card issuers will also notify you of chargebacks and will deal with any subsequent disputes.

Card Schemes

The card schemes provide the branding and infrastructure to enable credit and debit cards to be used internationally. The card schemes also provide rules for card acceptance and a mechanism for acquiring banks and card issuers to talk to one another during authorisation.

Visa/MasterCard Directory

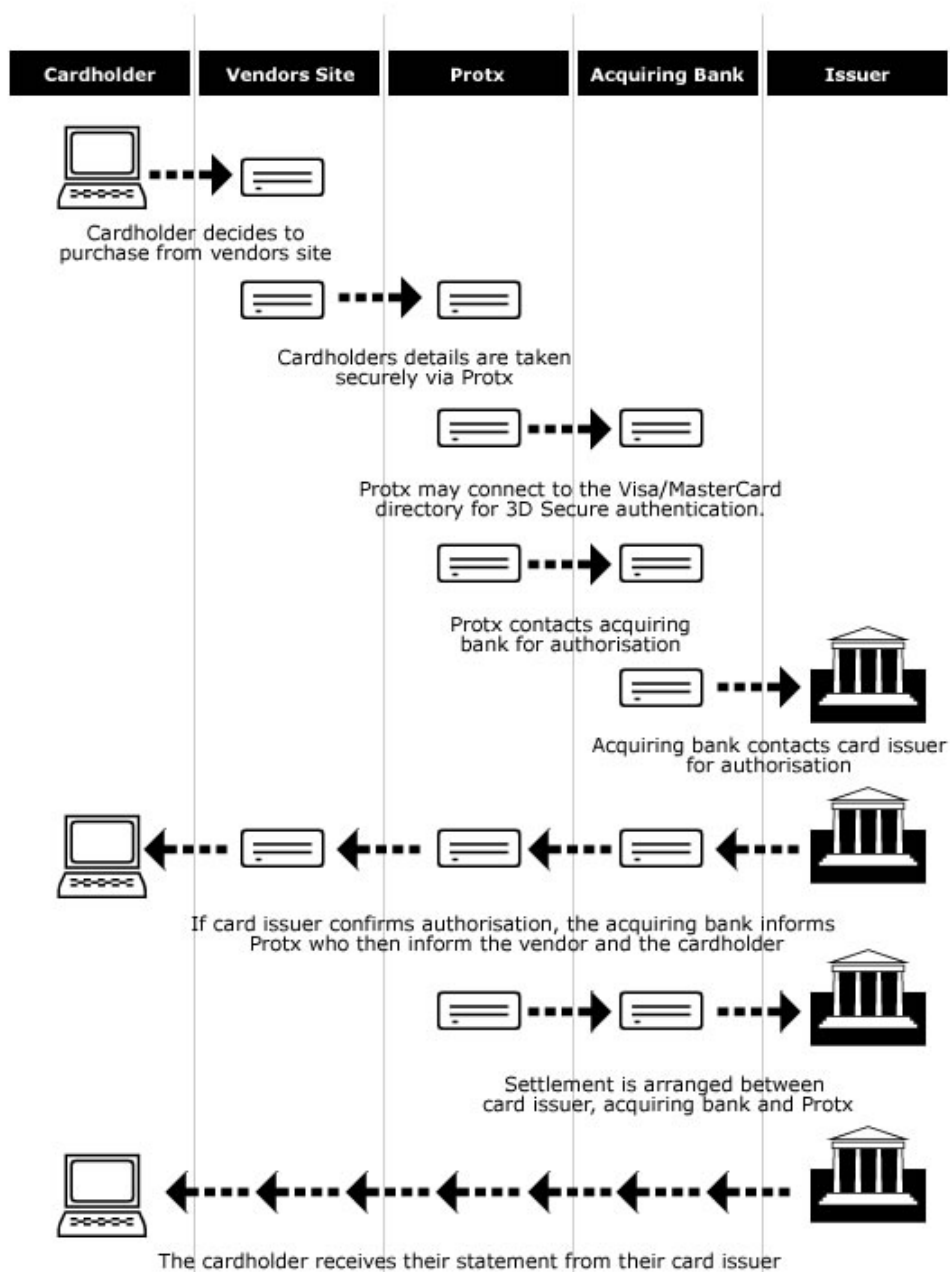
The Visa/MasterCard Directory provides information about each card and its current 3D Secure status.

Payment Service Provider

The Payment Service Provider (Protx) provides the software for merchants to take online credit and debit card payments in a secure environment. The Payment Service Provider software sits between the merchants acquiring bank and their website.



Transaction Process Diagram





04. Protx Fraud Prevention Tools

AVS/CV2

The banking industry introduced AVS/CV2 over three years ago to help combat the growing problems with verifying the cardholder during a CNP transaction. ProtX are fully compatible with AVS/CV2 across all acquiring banks. As a new vendor, you will have AVS/CV2 setup on your account by default.

Address Verification Service (AVS) – This allows you to check the numerics in the cardholders billing address with the card issuer. AVS is available for all UK issued Credit and Debit cards. AVS is not checked for overseas orders. The characters in the billing address are not checked as part of the AVS checks.

Important Note: It is possible for a cardholder to change their billing address details when they reach the ProtX site. If you would not like the cardholder to have the ability to change their address on the ProtX payment pages, you should change the templates setting in the Account Parameters section of your VSP Admin area.

Card Verification Value (CV2) – This allows you to check the additional 3 or 4 digit security code found on the signature strip on the back of the card. American Express cards have a 4 digit security code found on the front of the card just above the card number. CV2 can be checked on all cards issued within the EU.

Important Note : Although AVS/CV2 is setup on all new accounts, ProtX does not reject a transaction based on the AVS/CV2 response unless you have added AVS/CV2 rules to your account (see details on page 11).



AVS/CV2 Response from Protx

Protx will send an AVS/CV2 response in the AVSCV2 field for all transactions. The following responses can be returned:

ALL MATCH:	The numerics of the billing address and the CV2 matched with the card issuer.
SECURITY CODE MATCH ONLY:	Only the security code matched with the card issuer.
ADDRESS MATCH ONLY:	Only the numerics of the billing address matched with the card issuer.
NO DATA MATCHES:	Neither the numerics of the billing address or the CV2 matched with the card issuer.
DATA NOT CHECKED:	Either AVS/CV2 was not active at the time of the transaction, or the card issuer is unable to check the AVS/CV2 details at this time.

Also, if you are using VPSProtocol 2.22 you will receive the following fields which give a more detailed breakdown of the AVS/CV2 response:

AddressResult:	The specific result of the checks on the cardholder's address numeric from the AVS/CV2 checks.
PostCodeResult:	The specific result of the checks on the cardholder's Post Code from the AVS/CV2 checks.
CV2Result:	The specific result of the checks on the cardholder's CV2 code from the AVS/CV2 checks.

All of the fields can contain one of the following four responses:

NOPROVIDED
NOTCHECKED
MATCHED
NOTMATCHED

Important Note: You will only receive the detailed response for AVS/CV2 checks if you are using VPSProtocol 2.22.



AVS/CV2 Rules

AVS/CV2 Rules are not added to a Protix account unless you setup an AVS/CV2 rulebase in the Account Parameters section of your VSP Admin area. If you wish to perform your own manual checks on a cardholder, you should not use AVS/CV2 rules and refer to the Preauth and Deferred section in this document to enable delayed settlement of funds.

All acquiring banks (except American Express) now allow online reversals which allow Protix to apply an AVS & CV2 rule base to a Protix account.

An online reversal is simply the ability to reverse / cancel a transaction after the banks have authorised the card. Protix can cancel any transaction, based on the AVS & CV2 response from the card issuer. When the transaction is rejected, the transaction will be listed as Failed and the card holder will be informed on their screen and redirected back to your website.

Things you need to consider:

- UK Banks do not check foreign addresses so the response will be DATA NOT CHECKED or SECURITY CODE MATCH ONLY.
- Banks are not always able to check the AVS & CV2 data sent, if so the response will be DATA NOT CHECKED.
- Cardholders often type the wrong address in i.e. delivery address rather than the billing address or Top flat instead of flat 10.
- Cardholders may have moved and not changed the registered address with their card issuer.
- Delivering only to the billing address and getting a signature at the end reduces the risk of the items being passed to the wrong person.

For more detailed information about setting up a rulebase on your Protix account please refer to the following document

<http://www.protix.com/downloads/docs/protxrulebaseguide.pdf>



AVS/CV2 Rules and Manual Checks

You may want to combine AVS/CV2 rules with further manual checks on a transaction, especially when the AVS/CV2 response is Address Match Only or Security Code Match Only.

Ideally, you would only accept transactions which return All Match. In practice, this can mean that you are rejecting up to 40% of your orders. Some of these rejected orders may well be from genuine cardholders. If the AVS/CV2 response returned is Address Match Only or Security Code Match Only you may want to accept the transaction, but perform one of the manual checks detailed on page 20.

If you do not wish the customers card to be charged until you have completed these checks, you can use Deferred or Preauth to delay settlement of funds until you are happy with the transaction (see page 19 for details).



Verified By Visa and SecureCode (3D Secure)

What is 3D Secure?

The card schemes have developed more secure methods for authenticating the cardholder at the time of the transaction. These are called Verified by Visa (Visa, Delta, and Visa Debit) and MasterCard SecureCode (MasterCard, Maestro, and Solo); American Express, and Diner's Club.

VbV and SecureCode require the cardholder to enter a password during the transaction process. The cardholder will first need to register their password for VbV or SecureCode with their card issuer.

How does it work?

Visa and MasterCard will require cardholders to enrol for VbV and SecureCode via their card issuing bank. Card issuers may prompt cardholders to enrol at the time of the transaction, or may use a separate enrolment process.

Once the cardholder has enrolled, they will be prompted to enter their password whenever placing a transaction through a 3D Secure enabled site. The password is then sent to the cardholders issuing bank and checked against the issuing bank's systems. If the password matches, the cardholder is authenticated and the payment process continues in the normal way. If the password does not match it is possible for you to implement a rulebase to stop the transaction being sent to the bank for authorisation and therefore avoid a potentially fraudulent transaction from being processed. For further information about setting up a 3D Secure rulebase on your account please refer to our rulebase guide at <http://www.protx.com/downloads/docs/protxrulebaseguide.pdf>

How does the payment process work for 3D Secure transactions?

1. The cardholder decides to purchase with a MasterCard or Visa card from a 3D Secure enabled site with Protx.
2. The cardholder enters their card details and clicks the proceed button on the Protx payment pages.
3. Protx sends information to the MasterCard or Visa directory server. Protx queries the directory server to find out if the card issuer is participating in the relevant 3D Secure scheme and whether the cardholder has enrolled.
4. If the cardholder has enrolled, Protx sends a request for authentication to the appropriate issuing bank card.
5. The issuing bank displays a screen with their branding on to the cardholder who is prompted to enter their password.



6. The issuing bank sends the authentication results back to Protx.
7. If you have setup a 3D Secure rulebase on your account and the authentication results do not pass your rulebase, the transaction will not be sent to your merchant bank for authorisation. If you have setup a 3D Secure rulebase and the 3D Secure authentication result passed your rulebase, the transaction will be passed for authorisation. If you do not have a rulebase setup on your account the transaction will be passed for authorisation if the 3D Secure Result was OK/Fully Authenticated.

3D Secure Requirements

If you would like to use 3D Secure on your account, your site must meet the following requirements:

1. Your website must be using VSPProtocol 2.22, if you are using any other protocol it will not be possible to setup 3D Secure on your account.
2. If you are using cart software you will need to ensure that the software you are using is using VSPProtocol 2.22.
3. Currently 3D Secure is only available to merchants using VSP Form or VSP Server. Customers using VSP Terminal will never be able to use 3D Secure because the customer must be able to enter their password details at the time of the transaction. 3D Secure will be available to VSP Direct merchants in Q3 2006.

How to I setup 3D Secure on my Protx account?

If your site meets the above requirements, and you wish to setup 3D Secure on your Protx account, you should email support@protx.com with your Vendor Name in the subject line and your request to setup 3D Secure on your Protx account in the body of the message.

Checking the 3D Secure Authentication Result?

The 3D Secure authentication result is presented in your VSP Admin Area and in the 3DSecureStatus field returned to your site at the time of the transaction.

The 3D Secure authentication result is displayed in the Transactions section of your VSP Admin area in the format shown below. Any transactions with a green flag shown for the 3D Secure result have been authenticated and you will receive a liability shift on the transaction.

Please refer to the following table for a list of the results which can be returned for 3D Secure within the VSP Admin area.



Indicator	Message
	The Card is part of the 3D Secure scheme and authentication is available, but authentication did not complete. No 3D-Authentication occurred!
	The Card is either not part of the 3D Secure scheme or authentication was not available. No 3D-Authentication occurred!
	The 3D Secure network cannot determine if authentication is possible on this card. No 3D-Authentication occurred!
	3D-Authentication was attempted, but was not able to complete. No 3D-Authentication occurred!
	The initial authentication request was MALFORMED. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	The initial authentication request was INVALID. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	The initial authentication request returned an ERROR. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	The transaction FAILED 3D-Authentication.
	The authentication callback message was MALFORMED. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	The authentication callback message was INVALID. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	The authentication callback message returned an ERROR. No 3D-Authentication occurred! Please e-mail support@protx.com to inform us of this error.
	This transaction was fully 3D-Authenticated.
	3D-Authentication was attempted, was not completed, but a (C)AVV value was returned, so the transaction is Authenticated.

Transactions which have a 3D Secure indicator have been authenticated and you will receive a liability shift.

The 3DSecureStatus returned to your site at the time of the transaction can contain any one of the following 5 responses.

Response	Explanation
OK	3D Secure checks carried out and user authenticated correctly.
NOTAVAILABLE	The card used was either not part of the 3D Secure Scheme, or the authorisation was not possible.
NOTAUTHED	3D-Secure authentication checked, but the user failed the authentication.
INCOMPLETE	3D-Secure authentication was unable to complete. No authentication occurred.
ERROR	Authentication could not be attempted due to data errors or service unavailability in one of the parties involved in the check.

If the 3D Secure authentication result shows anything other than OK you should ensure that you consider this result along with the other fraud screening results for AVS/CV2 checks and The 3rd Man.

If you receive an OK/Fully Authenticated result, the AVS/CV2 results return all match and you have a low risk rating from The 3rd Man you have the best result possible for your fraud screening and you can be very confident that the person using the card is the genuine cardholder.



What is a 3D Secure Rulebase?

You should setup a 3D Secure rulebase if you wish to change the way in which 3D Secure results are handled by the Protix systems.

Without a rulebase setup on your account all transactions which return a result other than "The transaction FAILED 3D-Authentication" will be sent to the bank for authorisation. If you wish to stop transactions which return anything other than "The transaction FAILED 3D-Authentication" you will need to setup a 3D Secure rulebase.


For more information about setting up a 3D Secure rulebase please refer to the Protix Rulebase Guide at

<http://www.protix.com/downloads/docs/protixrulebaseguide.pdf>

A Change in Liability for Chargeback's

In the past the merchant has always been liable for chargeback's on their account. 3D Secure allows the merchant to shift the liability to the card issuer for certain transactions which are subject to a chargeback (the cardholder denies making the purchase).

The use of 3D Secure will enable you to shift the liability in the event of a chargeback to the card issuer under any of the following conditions:

- You receive an OK/Fully Authenticated result indicated by a 
- It is also possible to receive a liability shift for those transactions where the card issuer or cardholder has not enrolled. For more detail about this kind of liability shift you will need to contact your merchant bank.

Important: The use of 3D Secure will not remove liability for goods not received and disputes regarding the quality of the goods despatched.

For more information about VbV and SecureCode, please visit the following sites:



<http://www.visaeu.com/verified/>



<http://www.mastercard.com/securecode/>



The 3rd Man Fraud Prevention

Protx partner with The 3rd Man to provide a comprehensive risk management service exclusive to Protx customers.

Service Overview

The service provides Protx customers with a highly sophisticated fraud screening process to help detect and act on fraudulent orders before goods are shipped.

Each transaction is screened by The 3rd Man and the results are displayed in an easy to understand decision tool within the Protx VSP Admin reports alongside the AVS, CV2 and Verified by Visa and MasterCard SecureCode.

Each transaction is given a risk rating of high, medium or low, colour coded red, amber and green respectively so that merchants can see at a glance the level of risk associated with each transaction. A breakdown of the fraud score is also provided to give a detailed explanation of the rating including the results of the electoral roll, PAF file check as well as AVS and CV2.

The risk rating provides merchants with more information about the transactions they receive to allow them to make informed decisions about whether or not to accept the order.

The 3rd Man also provides a dedicated advice line to Protx merchants who wish to speak to a risk expert.

The fraud screening and decision tool have been provided free of charge as a special offer since November 2004. The advice line will be charged at 50p per minute to cover the costs of this support service.

The 3rd Man screens all available data and considers:

- Who is transacting?
- What are they buying?
- Where is it to be delivered?
- When was it ordered and when will it be delivered?

The 3rd Man analyses behaviour patterns to expose the risk factors:

- Multiple addresses used by same person or payment token or card.
- Repetitive names or addresses used.
- Similar names or addresses used.
- Repetitive payment token or cards attempts.
- Delivery to 3rd party or high-risk postal areas etc.



Many other dynamics are considered each of which is reported to you. You can look at the reports in detail or simply review our risk assessment i.e. High, Medium or Low.

The Fraud Screening Process

Data Submitted

- Protix will securely transmit all transactions processed in the previous hour to The 3rd Man on an hourly basis.

Data Screened

- The 3rd Man will then process the transactions through their suite of risk-management rules and perform an electoral roll and PAF (postcode address file) check. The electoral roll will validate whether the person is registered at the given address and the PAF whether the Royal Mail recognises the given address.
- The rules engine will screen each record by validating against lists of known bad and good cards, addresses, telephone numbers, email addresses and IP addresses and by executing rules looking for behavioural trends, patterns and abnormalities.

Preliminary Result

- All transactions will be screened as soon as they are received and a preliminary risk assessment will be notified to Protix. Once all the checks have completed, each record will be scored and allocated a risk category (Low, Medium or High) by analysing which rules have been broken.
- Low indicates that there are no significant risk factors within the transaction details. Medium indicates that there are some risk factors within the transaction details. High indicates that there are significant risk factors within the transaction details.
- Once all records have been processed The 3rd Man will pass a file containing the preliminary risk score, risk category and a complete list of the rules that have been broken to Protix.
- VSP Admin will be updated with the preliminary risk assessment to show whether the transactions are high, medium or low risk.

Continued Screening

- The 3rd Man will continue to screen and re-assess the transactions until the following day when a final fraud screening result will be provided. This makes use of all the time available before goods are actually shipped to continuously screen transactions to detect for fraud. This type of screening is highly effective in catching first time fraudsters.

Final Result

- At 04:00 each morning all the previous days orders will be re-assessed and a file containing the final risk score, risk category and list of rules that have broken is passed to Protix.
- This final assessment will overwrite the preliminary results in the Protix Admin screens. These results help merchants to decide whether or not to accept a transaction that is processed on their website.
- Hourly, Protix will automatically forward details of your transactions to us. We import this data and 'screen' each transaction against a set of rules that is customised for you.



Deferred and Preauth transactions

IMPORTANT INFORMATION REGARDING PREAUTHS

As of 1st November 2006 we can no longer provide the PreAuth payment type as an option to new Protx vendors. The PreAuth payment type will still work for existing vendors who already have the payment type enabled, but only until 31st May 2007.

As of 1st June 2007 the PreAuth payment type will no longer be a service that Protx provide. An alternative to the PreAuth payment type will be available, full details of this will be provided to all Protx vendors in January 2007.

You may wish to perform your own manual checks on the cardholder to ensure that they are genuine (see page 20 for details). After you have completed these checks, you can arrange for funds for each transaction to be settled on request as opposed to part of the automated process.

This allows you to perform manual checks on the cardholder such as address checks, STD checks, or credit status checks.

It is also useful to delay settlement if you don't always have the goods in stock.

The two options for delaying settlement of funds are:

Deferred: A deferred transaction shadows the card for the full amount of the transaction. The funds are not settled until you choose to send the release message to Protx to settle the funds. A shadow on a card will normally last up to 5 days. To be sure of receiving the funds, you should release the transaction within 5 days of the deferred transaction.

For more information about changing your website settings to make use of Deferred transactions, please refer to your integration documentation.

By default, no Protx accounts are setup for Deferred transactions. If you wish to setup deferred payments on your Protx account, please email support@protx.com

Preauth: A preauth transaction will not usually leave a shadow on the card. The transaction is cancelled and not settled until you send a repeat message. The repeat transaction requests authorisation from the card issuer again and the funds are settled in the normal way.

For more information about changing your website settings to make use of Preauth transactions, please refer to your integration documentation.



By default, no Protx accounts are setup for preauth transactions. If you wish to setup preauth transactions on your Protx account, please email support@protx.com

For more information about manually checking the cardholder's details to confirm that they are genuine, please see the manual checks on page 20.

Using Deferred or Preauth Transactions to avoid bank transaction fees

With a standard Payment transaction you will be charged a transaction fee by your merchant bank. If you decide not to fulfil the order (e.g. you don't have the item in stock) and therefore perform a refund, you will also be charged a fee for the refund transaction. To avoid being charged these transaction fees, you should use Deferred or Preauth transactions.



05. Manual Checks

When should you perform manual checks?

You may wish to perform manual checks on a transaction to ensure that the customer is the true cardholder. Normally, you would only need to perform manual checks on transactions if you are worried that the transaction may be fraudulent. Some fraud indicators are given below.

Possible Fraud Indicators.

- The value of the order is higher than you would normally expect
- The AVS/CV2 response is not ALL MATCH
- The order is from a country which is listed as high fraud risk, see below:
 - Bosnia
 - Bulgaria
 - Croatia
 - Egypt
 - Indonesia
 - Iran
 - Iraq
 - Israel
 - Malaysia
 - Nigeria
 - Pakistan
 - Romania
 - Russia
 - Serbia
 - Yugoslavia
- The customer has ordered more than once in a day
- The customer has attempted to make payment several times with the first few transactions failing
- The country of issue for the card does not match the delivery address
- The customer refuses to confirm their card details
- The customer alters the delivery address at short notice
- The customer demands next day delivery without regard for the extra costs involved
- The 3rd Man returned a high risk fraud screening result
- The 3D Secure Authentication result returned a yellow or red flag



What manual checks can you perform?

If your processes have flagged a transaction for further investigation, you may want to perform the following manual checks.

- Send an email to the email address supplied by the customer to confirm that it exists
- Check the area code of the phone number matches the address by using one of the free web based tools such as http://www.brainstorm.co.uk/uk_std_code_search.htm
- Check the customers name with directory enquiries http://www2.bt.com/edq_resnamesearch to verify the address against the telephone number
- Ring the customer on their landline number to confirm the order details and check that the telephone number and customer exist
- Check the IP Address of the customer at <http://www.iana.org/assignments/ipv4-address-space> to confirm that the IP Country matches the billing address. You will be able to find the customers IP Address in your VSP Admin screens



06. Other Fraud Prevention Advice

High Value and Overseas Transactions

High value goods and overseas transactions should be treated with extreme caution. You should consider delivery through a courier company who can obtain a signature upon delivery.

Delivery

Usually goods ordered via the Internet will be delivered to the customer. In some cases, the customer may collect the goods in person. If the customer does collect the goods in person, you should obtain a signature and ask the customer to show the card used during the transaction. You should then process the transaction as a cardholder present transaction and refund the transaction placed through the Internet.

You may want to consider the following:

- Only deliver goods to the cardholder's permanent billing address
- Avoid sending goods to hotels or guest houses
- Only send goods by registered or recorded post or by a reputable courier. Insist on a signed and dated delivery note
- Couriers should return goods if they are unable to deliver to the address specified

Transaction receipt

You should always provide a receipt to your customer. The on screen receipt should be printable and preferably an email should be sent to your customer on completion of their order. If you are using VSP Form, Protx provides a facility to allow you to send an email to your customer upon completion of the transaction.

VSP Admin

You should use your VSP Admin area to examine your transactions on a regular basis. You will need to look for fraud patterns as detailed previously. You may also want to consider using the 3rd Man fraud screening service which can perform these checks for you.

Important Note: It is possible for a cardholder to change their billing address details when they reach the Protx site. If you would not like the cardholder to have the ability to change their address on the Protx payment pages, you should email support@protx.com and request our address read only payment pages.



07. Additional card scheme requirements

Mandatory website content requirements

- Complete description of goods, e.g. if selling electrical goods you should state the voltage requirements
- Customer service contact information, including e-mail address and telephone number
- Return, refund and cancellation policy
- Delivery policy
- Country of merchant domicile
- Transaction currency or currencies
- Export restrictions

Additional website content requirements

- Privacy statements
- Details of what will appear on a cardholder's statement
- up-to-date stock information
- A transaction security statement

Protx Security Statement

You may wish to add a security statement to your website. We have given an example below; please feel free to use this on your website.

The Protx payment system uses a combination of established and innovative techniques to ensure the security and integrity of all sensitive data. Our internet facing web servers are certified by Verisign, this ensures that no third parties can impersonate Protx to obtain secure information.

Transaction Security

The transfer of the less sensitive transaction details from the retailer's site to Protx is encrypted and digitally-signed. This ensures that the information passed is secure and tamper-proof.

Security for the Shopper

Any communication between the customer and Protx is encrypted to the maximum strength supported by the customer's browser. The customer is also protected from fraudulent use of their card in a "card not present" environment, by their card issuer.

Data Storage

All data stored on Protx systems is held on encrypted and highly secured databases. Protx are regularly audited by Visa and MasterCard to ensure that their systems conform to the latest security standards.



08. The Chargeback Process

What is a chargeback?

Generally a fraudulent online transaction will result in a chargeback for which you (the merchant) will be liable, unless you have 3D Secure Authentication setup on your account. For more information about 3D Secure Authentication and receiving a shift in liability for certain chargeback's please refer to page 15 of this guide. A chargeback can occur for a number of reasons. The main reason is when the genuine cardholder reports an unknown transaction on their card statement to their card issuer. You may not be made aware of a chargeback until up to 6 months after the original transaction.

What happens?

You have 14 days to process a chargeback and will be required to provide all of the necessary paperwork related to the transaction. You will need to supply any details which can help you prove that the cardholder participated in the transaction. This paperwork can include receipts, details of telephone conversations, and any other correspondence which may be relevant. Once the card issuer has received the paperwork, they will investigate further. This will enable the card issuer to confirm if the cardholder did participate in the transaction.

If you don't receive any further contact from the card issuer that chargeback may be closed. However, if the chargeback does proceed, you will be required to provide further information to defend the chargeback.

After this process is complete, the card issuer will go back to the cardholder, obtain a response from them and then decide on the appropriate course of action. The onus of proof will always lie with you as the merchant.

You should contact your merchant bank for more information and a comprehensive explanation of their chargeback rules.



09. Top 10 Tips

1. Is the sale too easy? If the customer doesn't seem particularly interested in the product details it may not be a genuine sale.
2. If the goods you are selling are high value or easy to resell, you may be at higher risk of fraud.
3. Is the sale higher than you would normally expect, or for more items than you would normally expect?
4. Has the customer given a landline phone number? Most fraudsters will give a mobile number because it is harder to trace.
5. Is the customer using a friend or relatives card to place the order?
6. Has the customer tried to order unsuccessfully on previous occasions?
7. Has the delivery address been used before with different card details?
8. Does the customer have problems remembering their address or order details?
9. Is the customer using more than one card to split the value of the order?
10. Is the customer requesting a refund via cheque?



10. Glossary of Common Terms

Acquiring Bank	The bank who obtain financial settlement from card issuers on behalf of the merchant
Authorisation	The process of authorising a card to be used for a particular transaction
AVS	Address Verification Service allows a merchant to check the numerical digits of the billing address of the cardholder during the authorisation process
Card Issuer	The bank who have issued the card to the cardholder
Card Schemes	The card schemes set the business rules that govern the issue of the payment cards that carry their logo. In the UK, banks and building societies must be members of the appropriate card schemes to issue cards and acquire card transactions.
Chargeback	A chargeback is a transaction which has been disputed by the cardholder. The card issuer will raise a chargeback with the merchant.
CNP	CNP (Cardholder not present) transactions are transactions where the cardholder is not present with the retailer at the time of the transaction.
CV2	CV2 (Card Verification Value) or CSC (Card Security Code) is the three or four digit code found on the card and is used to help confirm that the customer is the genuine cardholder
MasterCard SecureCode	The new initiative from MasterCard to help merchants verify the customer is the genuine cardholder and shift liability to the card issuer
Merchant	The company or person who has a merchant account with an acquiring bank to process card transactions
Verified by Visa	The new initiative from Visa to help merchants verify the customer is the genuine cardholder and shift liability to the card issuer
3D Secure	The general term for the authentication programs offered by Visa and MasterCard,