

Managing Online Fraud – A Merchant's Guide to Best Practice



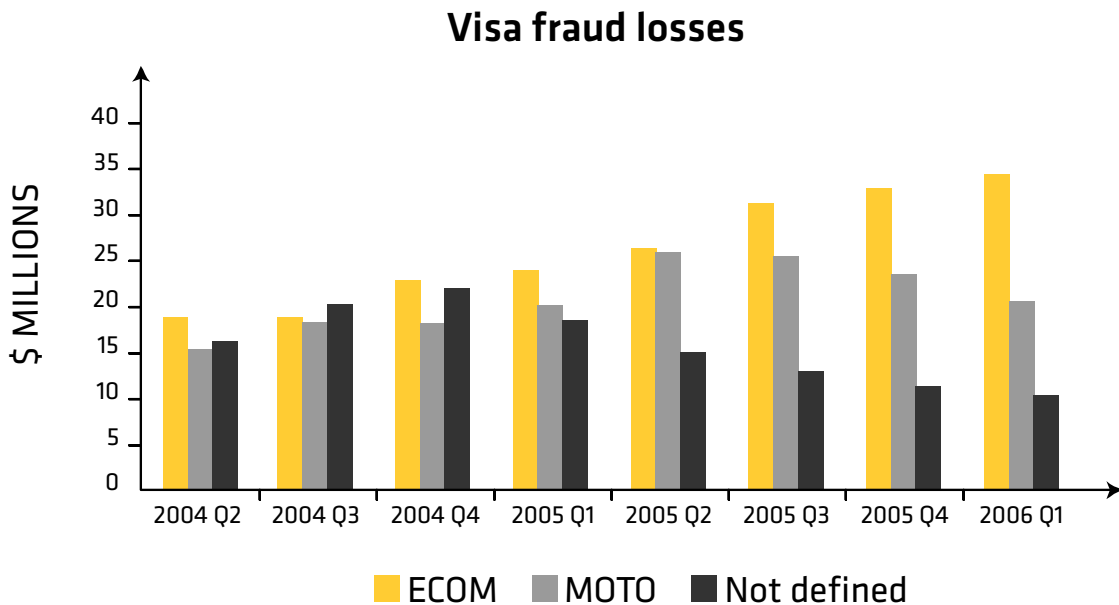
1. Payment card fraud – what is it?

The term “payment card fraud” occurs almost daily in the media today. The average reader is flooded with breaking news about new scams invented by increasingly cunning fraudsters. The general consensus is that it is getting more and more unsafe to use your payment card for shopping. This White paper deals with payment card fraud on the Internet, also referred to as Card Not Present fraud (CNP). It is called Card Not Present to distinguish it from a brick and mortar business where customers are required to have their payment cards present when paying. This is of course not possible when shopping online.

CNP fraud hits the e-commerce merchant, cardholders and the card issuing banks. Who gets to pay after the fraud is committed depends on several factors. Suffice to say that it is **not** the cardholder, contrary to popular belief. This topic will be covered later on.

1.1 Increase in online fraud in Europe

The fraud trend among European e-commerce sites continues to steadily increase. Between 2004 and 2006 the mail/telephone order industry has experienced a drop in fraud, while web shops have suffered an increase in fraudulent transactions. Since the first quarter 2004 till 2006, the dollar amount lost to fraud has doubled to a staggering \$35 million per quarter.



Source: Visa Europe



1.2 Phishing, carding, skimming etc.

A fraud requires two basic steps:

- 1) An action where the fraudster steals a card or illegally copies card information
- 2) An action where the fraudster uses the stolen card data to place an order online

Action #1 tends to get more attention than the actual illicit purchase attempt. The terms skimming and phishing are two ways of obtaining payment card details for fraudulent use at a later date. Skimming is when the fraudster swipes a payment card through a skimming device (picture). The card data is stored in the device and can be uploaded to a computer. The fraudster also needs to manually write down or memorise the CVV2 code found on the reverse side of the card.



Picture 1: A Skimming device

Phishing is a collective name for various illegal activities aimed at collecting passwords, payment card details or bank account details by masquerading as a trustworthy entity in an electronic communication. A fraudster can also *hack* a server that stores payment card data, thus gaining access to thousands of payment card details. However, one of the most serious threats to payment card integrity is insider leaks. For example, a disgruntled employee within a company handling payment card details can copy them and sell them for a profit (or use them for fraudulent transactions).

Card details (not the physical cards) are later sold or shared among fraudsters. The going price for a "virgin" card number, i.e. never used for fraud, is approximately between \$5 to \$10, CVV2 code included.



2. Description of Fraud

At this point the fraudster has a set of payment card details that are ready to use for online shopping. The main challenge for the fraudster is that he/she doesn't know the credit limits of the card or if there are sufficient funds on it. Furthermore the fraudster is under time pressure; the legitimate cardholder might have discovered what is going on and block the card through the issuing bank. The fraudster must act quickly to exploit the card numbers at hand.

- 1) The fraudster needs a delivery address, a.k.a. a "drop". This could be the private address of the fraudster, but professionals tend to use somebody else's. This address acts as a safety buffer and the person receiving the goods is simply a paid hand or a "fence".
- 2) The fraudster picks a web shop and enters bogus customer data, but uses a genuine address.
- 3) On the payment details page, the fraudster enters the payment card data. If the payment card account is active and funds are sufficient, the transactions will be authorised.
- 4) The product is dispatched and the fraudster signs the delivery slip upon arrival, using a fake ID if it is requested at all. Express delivery is the preferred method as it cuts the turnaround time, making it more difficult to detect and stop.
- 5) The legitimate cardholder, who could be living in a different country, discovers the purchase and initiates a charge back. The web shop that sold the product (and accepted the payment card) will normally *1) be held liable for the financial loss.

Encouraged by this success, the fraudster is likely to push his luck by placing more orders with the same company. This happens between item 3 and 4 in the process described above.

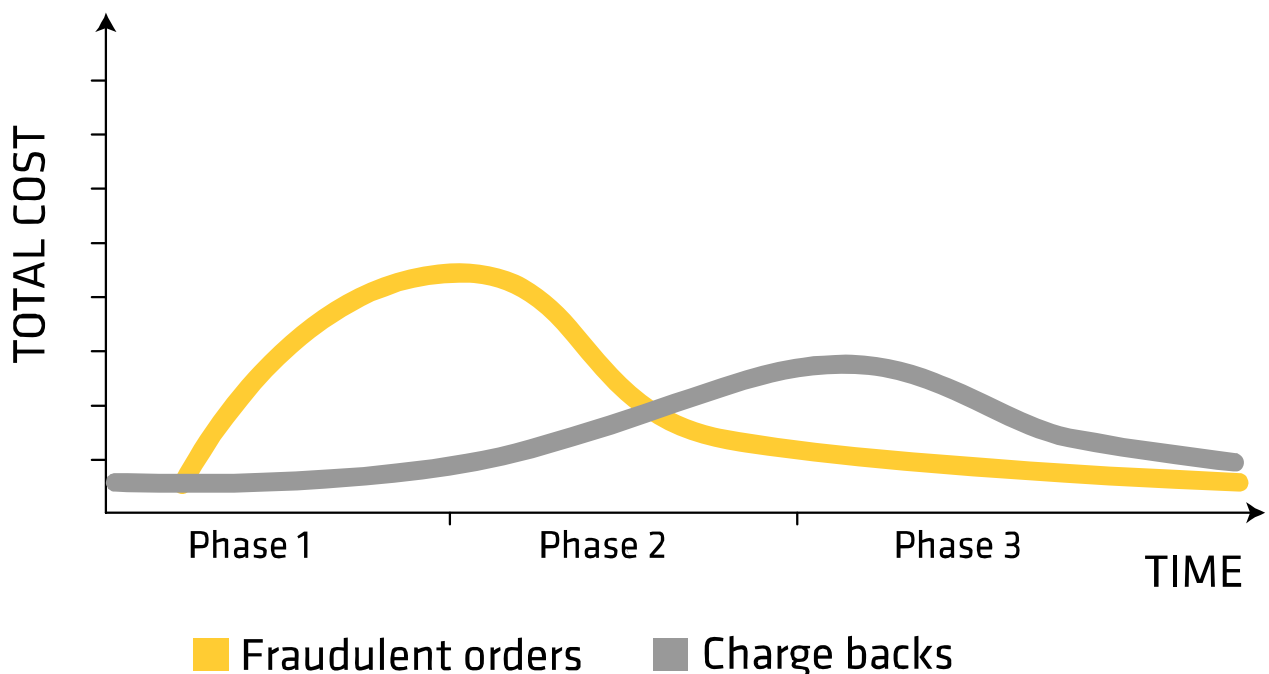
**1) The presence of 3D Secure/Verification programmes shifts the liability to the issuing bank, provided the merchant authorises the transactions according to it.*



3. Impact on Your Business (The Fraud Cycles)

All too often a merchant starts an online business without ample fraud protection. Typically, all focus is on marketing, IT infrastructure and the payment gateway. While the merchant without an active fraud prevention system might enjoy a grace period, it is just a matter of time before a fraudster discovers the site. As described above, the fraudster will not be content with just one or a few products; he will ruthlessly exploit the merchant and possibly share information about the vulnerable e-commerce site with other fraudsters. The result is a massive fraud attack.

Initially (*phase 1 in the graph below*) the merchant will be pleased to see that business is booming, thinking that the fraudulent transactions are genuine orders. The core problem is that the legitimate card holder might not discover that his or her card data is corrupt. Maybe he or she is slack with checking the bank statement (normally sent on a monthly basis) or simply overlooks the fraudulent transaction among all other transactions. The average time span between a fraud being committed and the cardholder issuing a charge back is 2.5 months (approximately 80 days). Some card holders are quick to report fraudulent use of their cards, but an average merchant should expect a 2-3 months lag in the fraud/charge back cycle.



Graph 1: The Phases of a Fraud Attack



The first indication that something is wrong is a steady but increasing charge back rate (**phase 2**). When examined, it becomes obvious that the very same customer that placed the charge backed order has made multiple purchases over a brief period. Many of the transactions have been made with different payment cards. When analysing the transaction log the merchant also notices a very high number of denied orders during a short time span. This is followed by one or more successful orders. The merchant will also notice that the same payment card number appears with seemingly different customers.

At this point the merchant initiates an emergency plan. All incoming orders are usually vetted manually, and if there is any doubt, the merchant will deny the order and stop delivery of the goods ordered (alternatively freeze customer funds). All suspicious accounts are closed and an ad hoc “Black list” of names and addresses is created. Preventing fraud now has top priority and the negative impact on sales (due to stricter screening) is ignored. The fraud rate drops fast. The merchant quickly learns to reject a suspicious order and this has repercussions on the fraudster’s behaviour. As almost all their order attempts are rejected, and their accounts closed, they realise that they are discovered. Normally, the fraudster/fraudsters will move on to another e-commerce victim.

The merchant will now have to reset the priorities; fraud protection is now considered a key success factor and the merchant will look for a professional vendor of fraud protection services. However, it will take some time before the service is integrated and tuned to the merchant’s needs. All this depends on several factors, mainly technical.

In **Phase 3**, the situation is stabilised, but at a high cost. Fraudulent transactions have dropped, and the merchant now has one or several employees vetting all orders manually. The overall denial rate is high, as the credit team is instructed **not** to give a suspicious order the benefit of doubt. The credit team now operates under make shift “business rules”, meaning that they will single out certain products, orders above a certain price or some other combination considered risky. These rules can be automatically implemented by in-house IT development.

However, the merchant’s problems are far from over. Now all the cardholders will start to file charge backs, as they slowly begin to realise that their payment card data is corrupt. The charge backs will peak around 2-3 months after the initial fraud attack. Large parts of the revenue generated in phase 1 is now lost.

So far, the merchant’s problems have been limited to financial, operational and loss of good will. As the charge backs increase, the acquiring bank will take action (or the Payment Service Provider). Normally the acquirer monitors the charge back rate and has early warning systems that will detect when the charge back rate deviates from the normal. The acquirer can and most likely will simply terminate the merchant’s contract. This effectively puts the merchant out of business, as no more payment card transactions can be processed.



3.1 Analysis

The scenario described above poses some serious threats to the e-commerce store. Firstly, there is the pure financial loss, i.e. goods/services shipped but not paid for. Secondly, there is the lost sales impact and the loss of good will as the merchant launches the emergency plan, causing more rejected orders. Finally, the loss of acquiring contract may lead to the collapse of a business, especially if the merchant only has one acquirer.

It must be stressed that the merchant needs to have a fraud strategy from day one. Therefore a key factor is to make Phase 1 as short as possible. The merchant needs to take immediate action when fraudulent activity is noticed. Furthermore, the countermeasures taken must ensure that normal business flows uninterrupted. A professional anti fraud service provider should be hired and be given priority. The merchant also needs to be proactive in dealing with the acquiring bank. This includes proving that they have an action plan to fight fraud and that there is a fraud strategy in place.

3.2 Aftermath (Post Phase 3)

As the last of the charge backs trickle in and the merchant has installed a fraud prevention system, the merchant usually considers the problem solved. Now the focus will shift to reclaiming lost market shares and expanding the business. As this happens (usually 4-6 months after the fraud attack) the merchant faces conflicting forces: The Sales department will fight for reduced credit and fraud rules and the Credit department (or equivalent) will try to keep the fraud rate down. In this battle, the sales department will usually come out as the victor. A higher risk exposure is tolerated to promote sales. The fraud prevention system is relaxed. The stage is set for a second fraud attack and the whole process will be repeated again, usually with less severe consequences as the merchant has now gained some experience with fraud and can act quicker.



4. The Cost of Fraud

The cost of fraud covers more than just the actual goods shipped or services consumed. As briefly mentioned in the previous chapter the cost can be divided into the following categories:

- 1) **Financial loss:** Goods/services delivered and later charge backed.
- 2) **Loss of Goodwill:** Card holders will blame the company for the fraud.
- 3) **Administrative costs:** The bank charges a fee for each charge back handled (approx \$30 USD).
- 4) **Staff costs:** The merchant has to allocate resources to manually screen incoming orders and the finance department has to administrate refunds and charge backs. The merchant's customer service department will receive numerous calls from card holders subject to fraud.
- 5) **Fines:** The merchant can get a substantial fine from VISA/MasterCard (passed on to the acquirer) if the charge back rate goes above a certain percentage (normally 3% of the turnover).
- 6) **Lost Sales:** By imposing stricter fraud rules, good business will be turned away as it is difficult to distinguish good orders from bad orders. The quality of the fraud prevention service is important in keeping this cost low. Furthermore the customer experience when shopping is important, if there are too many security measures in place the customers might be discouraged to shop on the site.

The most difficult part is to balance the charge back rate with lost sales. This topic will be covered more thoroughly in the next chapter. As costs associated with fraud are cumulative it is imperative to find a best practice in managing them. Priority should be given to keep the charge back rate under a pre-defined percentage, as this is the main cost driver. Although the merchant might be able to absorb the financial costs, the fines for exceeding the limit can drive the merchant to bankruptcy.



5. Optimising Fraud Costs

This White paper has stressed the importance of keeping fraud checked and to minimise the costs driven by it. Should then an e-commerce merchant opt for a zero tolerance strategy against fraud? **The answer is no.** Contrary to popular belief, the ultimate goal of a fraud prevention strategy is not to keep the fraud rate at naught percent. The rationale behind this is simple: the cost of lost sales (resulting from stricter Fraud Prevention System settings) would be greater than the cost of goods lost to fraud. In other words, as the merchant applies tighter security settings in an attempt to eliminate all fraud the alternative costs will rise. These costs include lost sales and staff costs.

One popular and effective method of safe guarding against fraud is to create a credit team dedicated to reviewing orders manually before releasing them. This is common among high end product industries, such as expensive electronics equipment suppliers. As the amount of orders increase, the merchant has to employ more resources to the team (or pay them to work overtime), and the staff costs increase. The conclusion is: once the merchant has stabilised the Fraud rate (i.e. the charge back rate) the question needs to be asked: *“how much did they spend on achieving that charge back rate?”*

The following figure illustrates three cases. Each case represents a fraud prevention strategy and the effective, combined cost.

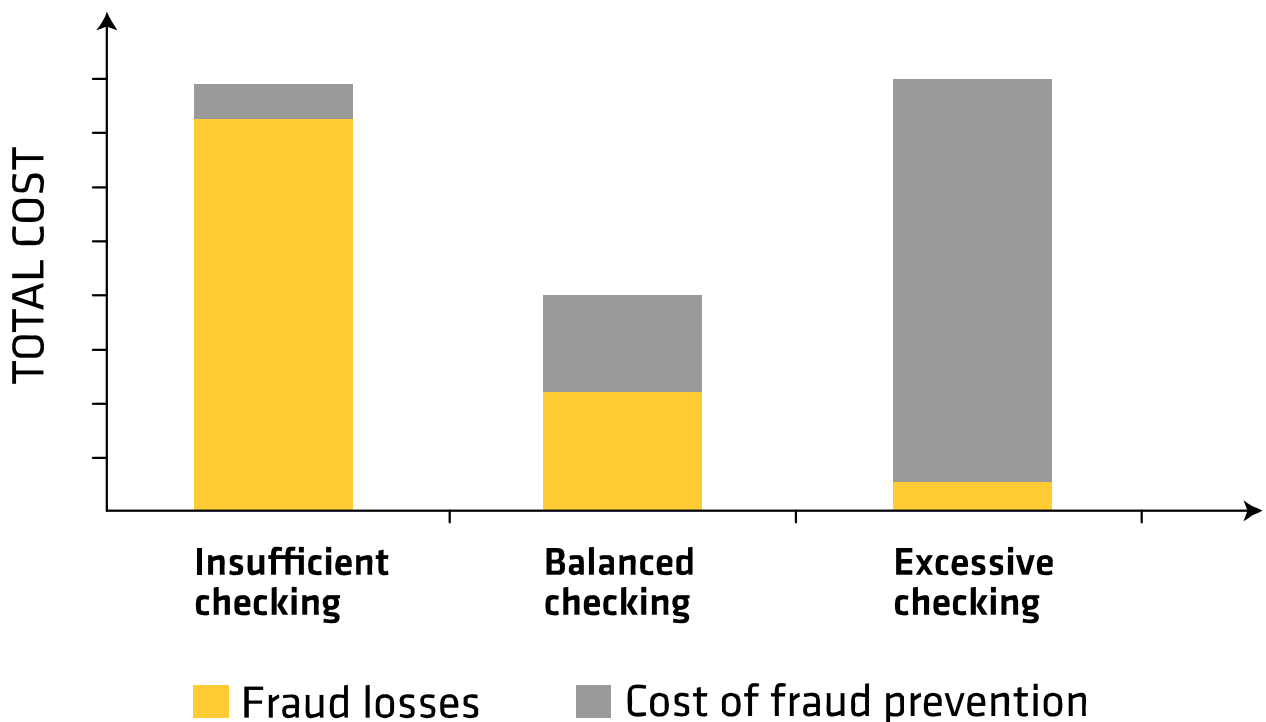


Figure 1: Minimising the total cost of fraud. The labels indicate the percentages of orders reviewed and fraudulent orders in each of the three scenarios.



The chart in Figure 1 shows the total cost of fraud as the sum of the actual fraud losses, plus the cost of preventing fraud. The left column shows a scenario where fraud losses dominate the total cost, because of **insufficient fraud prevention**. The right column shows the opposite extreme – an excessive amount is spent on a fraud prevention system and stricter settings. This results in fewer fraud cases but a substantial cost of maintaining the fraud prevention system and a high volume of lost sales. While fraud losses are no longer an issue, the cost of achieving this result is not acceptable.

Finally, the middle column shows the optimal scenario – minimised total cost with acceptable fraud prevention cost and “residual” fraud losses. The example shows an overall result with a significant reduction in the *total* cost of fraud.

5.1 Lessons Learned

By now it should be clear that the key word is *optimising* not *minimising* the fraud costs. It helps if one takes an overall approach to the whole problem rather than just focusing on the fraud losses. Remember that: True cost of fraud =

Cost of fraud losses + cost of rejecting good orders + cost of fraud management (manual reviews included)

While some merchants are ignorant to the whole problem, others feel secure thanks to the Cardholder authentication programme, known as Verified by Visa and MasterCard secure code, also known as 3D Secure. This scheme launched by Visa/MasterCard shifts the financial liability from a merchant to the card issuing bank. In theory, the merchants participating in the 3DS could then ignore fraud losses, as they will not have to pay for them. However, there are constraints with the system, mainly one prerequisite being that the merchant keeps the fraud rate (Charge back rate) under one percent. The issue is then how to optimise the costs to achieve that target.



6. Implementing a Fraud Prevention Strategy

A Fraud Prevention Strategy differs from a Fraud Prevention System. A strategy is the combined set of tools, policies and targets aimed at keeping losses incurred by fraud as low as possible at the lowest possible cost. A Fraud Prevention System, or Anti Fraud System, is a set of tools integrated in a merchant's order process that will detect and stop a risky transaction. The latter should form the core component in the strategy.

Before implementing an Anti Fraud System (AFS), some key strategic decisions need to be made. The merchant needs to decide on a "Risk appetite", i.e. how much fraud exposure he or she is willing to accept by relaxing the anti fraud settings. The underlying idea is that by relaxing the AFS settings, more orders will be accepted. This could be important during a marketing campaign or in a start up phase. The key performance indicators should be:

- Rejection rate = the amount of orders rejected by the AFS compared to total orders.
- Chargeback rate = the amount of chargeback orders compared by total orders alternatively the chargeback cash value compared to total turnover.
- Amount of orders referred for manual review.

Best practice in this case would be to have the AFS rejections under 10%, preferably 3-5%. This is the expected rejection rate and is comprised by fraudulent attempts and false positives. Occasionally, this percentage will spike, due to fraudulent activity. This should be taken as an indicator that the AFS is actually working.

The chargeback rate is not usually communicated to the merchant by the acquiring bank. The merchant should try to get this important statistic. However, one thing is certain: should the chargeback rate go up, the acquiring bank will take action, as described earlier. This means that best practice in this case is to start off with a fairly strict AFS setting, and then gradually relax it. In practice many merchants operate under different conditions, like different geographical markets, and different product lines. The AFS settings should be adapted according to the estimated risk for those categories. For example, a European merchant might opt for stricter settings for non European transactions, while keeping the settings for domestic transactions at a minimum.

The amount of reviewed orders has been thoroughly discussed in the previous chapter. It is a quick solution to sudden fraud threat, but is not cost effective. Studies show that approximately 80% of the orders reviewed manually are later approved. The bottom line is: keep it at a minimum and try to rely on automated, online checks.

6.1 Customer Handling

A solid strategy in fighting fraud involves the whole organisation. Departments and resources should be adequately trained and informed about the basics of the installed Anti Fraud System. When the AFS becomes operational, a certain amount of transactions will be rejected. From a customer point of view this is a sensitive phase. A rejected, non-fraudulent



transaction will upset the customer and cause alarm. The reason for this is simple. The customer could be a first-time shopper, and is generally cautious about sharing payment card information on a Web page. Some countries are more accustomed to online shopping (USA, UK) while citizens in the Scandinavian countries have adopted a more conservative stance, preferring other payment methods than payment cards.

When a customer gets rejected, the following thoughts typically cross their minds (in a random order):

- 1) Why was my payment card rejected?
- 2) Was money drawn from the card?
- 3) Should I try again?
- 4) Whom do I call to get support?

All this anxiety will be aggravated if the online message displayed when the transaction was denied is brief and blunt, like “Your transaction has been stopped/cancelled” or “Transaction aborted”.

The customer service department will suddenly get phone calls from rejected customers. It must be stressed: **the call centre staff must know how to deal with these calls**. If they do not know what caused the denied order, the customer will get the wrong information (or no information), which will result in a negative customer experience. The rejected customers calling are either cheeky fraudsters or genuine customers. It is difficult to distinguish between these two, and we do not recommend that the call centre staff should have a fraud screening function.

Best practice in this case is to train the customer support function to recognise the message that was displayed and to take appropriate action. The supplier of the AFS normally has a set of predefined messages that can be displayed. The messages should convey as little as possible of the reasons for the denial yet be informative and reassuring enough that the customer knows what happened and what to do next.

6.2 Tools in Fighting Fraud

The following tools are examples of procedures used in various fraud prevention systems by merchants today, listed in order of popularity:

- AVS - address verification system. The customer’s post code is matched with the customer data at the card issuing bank. If there is a mismatch the AVS will issue a “no” code, enabling the merchant to reject the order. AVS is a relatively old system that has some serious drawbacks; mainly that it is difficult to update directories when cardholders move to a new residence. This results in many “false positives”. AVS is available in the U.S. and U.K. (partly) only. It continues to be frequently used by U.S. merchants.
- Manual review. Described in previous chapters. Can be cost effective for merchants with low turnover and/or expensive products.
- Card Security Code (AKA CVV2, CVC). Introduced in 2002-2003 this three digit code printed on the reverse side of the payment card is unique to that particular card. It is



not stored in the magnetic strip. When shopping online, the customer is prompted to fill in the code with the card account number. The code is matched with the card and a negative response should be rejected. This code was introduced to stop generated card numbers and proved an efficient method of reducing online fraud.

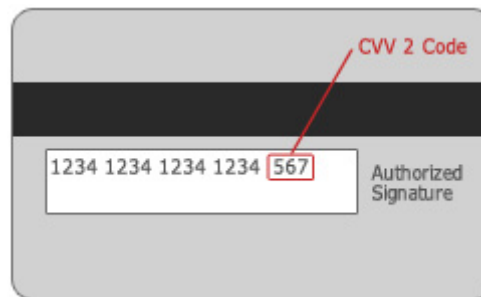



Figure 3: the CVV2 /CVC Code

- Blacklists/Whitelists. The merchant stores customer data and matches incoming orders with them. If part of the customer data (such as telephone number or address) is on the black list, the order is rejected, or referred for manual review. The white list is a reversed function, based on a positive customer relation. The main drawbacks with these lists are that they are cumbersome to maintain and often outdated. Furthermore, fraudsters frequently change their customer profiles, rendering blacklists useless.
- In-house fraud rules: A set of “business rules” enforced by the merchant. These are described in chapter 3 under “phase 3”. They provide crude but effective damage control as they are designed to stop the financially most harmful fraudulent transactions. The prerequisite is manual review; otherwise the lost sales will increase to an unacceptable level. Some geographical rules can be applied automatically for example rejecting all orders from a certain country.
- Verified by Visa /MasterCard Secure Code: This authentication programme helps in reducing liability for repudiation chargebacks, i.e. when the cardholder denies making the recorded transaction. These programmes require that cardholders who have previously registered with the schemes enter a password when purchasing goods from a participating merchant. The issuing bank then validates the password and authenticates the cardholder. VbV and MSC is years from full implementation and merchants will have to have additional procedures in place.
- Commercially developed Anti Fraud Systems. These systems of software are a bundle of services and checks carried out by a third party service provider specialised in Fraud Management. The technical solution differs slightly; in some cases the merchant can send the transaction data to the service provider who returns a reply code. This code often comes back in the form of risk scoring. Another solution is a built in payment gateway which performs the same screening and rejects or approves an order before authorising the transaction. These screenings are online and take less than a second. The service provider utilises sophisticated software that checks hundreds of different



aspects of the order. The combined assessment is matched against accumulated data on previous fraudulent behaviour. The system is then able to generate a risk scoring (usually between 1 and 10). The merchant can then choose the preferred risk level, as mentioned earlier. These systems also come with an option of setting business rules and geographical constrictions through an online graphical interface. The merchant may at any time change the risk settings.

Settings - Card issuing and IP countries

 **Card issuing and IP country block**
There are some countries that are masked by the networks as high risk countries. IP address or billing address in Egypt, Ghana, Indonesia, Lebanon, Macedonia, Morocco, Nigeria, Pakistan, Romania, Serbia and Montenegro, Ukraine, or Vietnam may be a risk.

There are also some card issuing countries and regions that are not participating in the 3D Secure program. Therefore we strongly recommend you to accept payments, only in those countries you are active in. If your customer base is global; we recommend you to block high risk countries and non-3d secure participating countries. [Click here for a list](#)

Important!
The transaction will be **processed**, only if the card is issued or if the customer's IP is located in your list! There are some issuers with too few cards to have a own BIN number, they may be placed under another bank's BIN and Country which may results to a non-100% accurate country check.

Please select mode: **1**

 Perform IP-BIN Cross check

Add a country to your **white** list: **2**




Status	Country	Added	
✓ 	Sweden	2005-12-21 14:18:59	Delete
✓ 	Denmark	2005-12-21 14:18:59	Delete
✓ 	Norway	2005-12-21 14:18:59	Delete

Figure 4: Example of a web based settings page. The merchant has selected Sweden, Denmark and Norway as eligible countries. Transactions from other countries will be blocked.



7. Conclusions

Card not present fraud is an ever present threat that will increase and become more sophisticated. If left unchecked, it can seriously harm a merchant financially and cause a revoked acquiring contract, which effectively terminates the merchant's means of getting paid. It is not advisable to try to eliminate fraud completely, nor should it be ignored completely. Fraud needs to be managed, just like any other business activity. A well managed and efficient Anti Fraud System together with a Fraud strategy is the best way to deal with it. Remember that your company does not necessarily have to be top class in fraud prevention. It simply needs to be better than your competitors, as fraudsters are more likely to target them instead of your business. A professional service provider of Anti Fraud Systems is an integral part of online business and can provide crucial advice before starting up an online business as well as supplying the tools needed to combat fraud.

About Samport

Samport specialises in helping banks, large merchants and system vendors make sure they can handle the demands on secure, effective and cost efficient transactions, whether through payment over the Internet or in retail stores. We make this possible through our two market leading products; Samport LETO and Samport ZEUS.