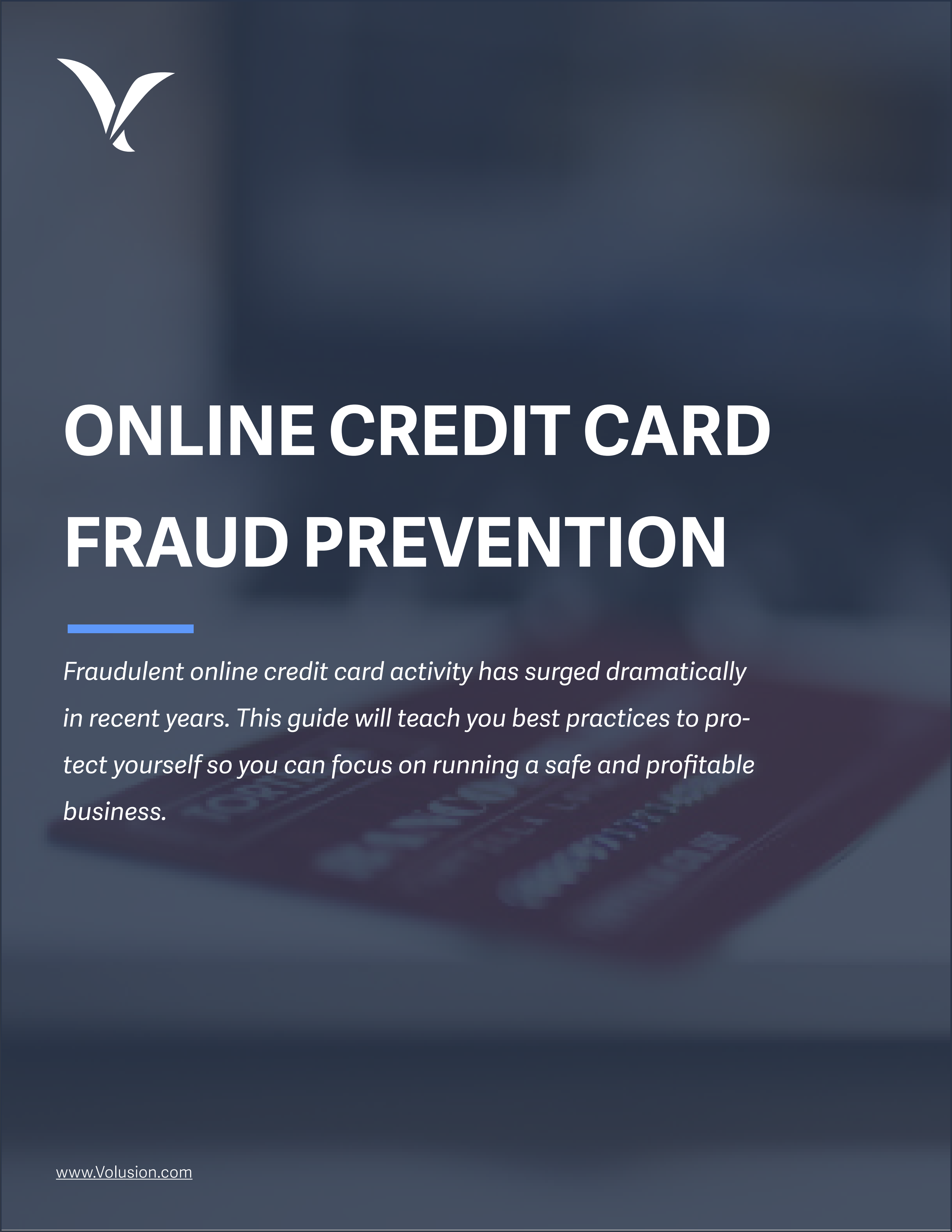


ONLINE CREDIT CARD FRAUD PREVENTION

Fraudulent online credit card activity has surged dramatically in recent years. This guide will teach you best practices to protect yourself so you can focus on running a safe and profitable business.

www.Volusion.com

1. Card data theft

Card data theft is a serious concern in ecommerce, more so than physical card theft.

2. The merchant is liable

The burden of financial liability is usually placed on the merchant who accepts the card.

3. Chargeback fees

Merchants are often assessed a chargeback fee in the event of a fraudulent transaction.

4. The impact of chargebacks

Chargebacks can impact inventory levels, short-term revenue and much more.

5. Minimize the risk

Fortunately, there are many effective fraud prevention methods available to merchants.

Fraudulent online credit card activity has surged dramatically in recent years. Without widespread merchant complacency and lack of awareness about how fraud works, this phenomenon would not have been possible. After all, no one would find stealing credit cards to be worth the time and effort if no merchants honored them for payment. It is unfortunate enough that many merchants do not understand how fraud works and the part they play in its success, but it is even more unfortunate that many merchants do not realize how fraud can impact them until it is too late. Contrary to what many uninformed merchants assume, credit card fraud is primarily a problem for merchants, not cardholders. As long as data security standards remain incapable of eliminating fraud outright, education is essential for self-protection. Below you will find key facts to keep in mind, as well as best practices to follow.

Internet transactions, like all “card-not-present” transactions, are inherently more susceptible to fraud than “card-present” ones.

There are two basic kinds of credit card theft. The first is the obvious, old-fashioned kind in which the card is physically stolen. The second (and more common) kind is the covert separation of the data from its card. In either case, the rightful cardholder can thwart fraudulent purchases by simply contacting the issuer and requesting cancellation; the issuer then immediately declines all subsequent authorization attempts. In a transaction environment that requires the physical presence of the card, such as a retail store, card theft is of minimal concern. It may be possible for a fraudster to use a physically-stolen card, but this rarely happens because of the relatively short average window of time between theft and detection; most cardholders notice and report physically-missing cards within 24 hours. And purchases with compromised card data are of practically no concern at all, since producing a counterfeit card with stolen data (functional magnetic stripe and all) is usually far more trouble than it is worth.

On the other hand, in a transaction environment that uses card data as a substitute for the physical card, such as the internet, it can be challenging for merchants to spot the difference between a rightful cardholder making a legitimate purchase with the physical card, and a fraudster making an illegitimate purchase with stolen card data. Therefore, even though physical card theft is no more of a concern for online purchases than it is in card-present environments, card data theft is a serious concern in ecommerce.

If cardholders were able to notice and report stolen data as easily as they are able to notice and report a physically missing card, data theft would not be much of a concern even in and report a physically missing card, data theft would not be much of a concern even in card-not-present environments. Unfortunately, cardholders usually do not learn that their data has been stolen until they notice one or more unfamiliar charges on their statements. And since many cardholders do not monitor their statements regularly or closely, weeks or even months can pass before a compromised card is canceled. In the meantime, issuers authorize all otherwise-unsuspicious transactions, and unsuspecting merchants become saddled with harmless-looking fraudulent orders. While it might seem reasonable to assume that the cardholder, the issuer, the processor, or the gateway loses out in these situations, that assumption is incorrect.

Industry standards established by the card brands specify you, the merchant, as the financially liable party in most cases of card-not-present fraud.

Since cardholders, issuers, processors, and gateways are powerless to detect and prevent most cases of online credit card fraud, the card brands place the financial liability on the merchants who accept the cards. If this seems unfair, it is important to understand that merchants possess more fraud prevention leverage than any other party involved in an online credit card transaction. Banks perform their duties on the assumption that merchants are aware of this. Unfortunately they often are not.

It is important to remember that capturing funds is always a matter of choice for the merchant. Many merchants feel safe capturing funds on all

authorized transactions because they mistakenly assume they cannot be held responsible for processing a fraudulent transaction. After all, they did not steal the card and another party (the gateway or the issuer) “authorized” the transaction. Do not let the name of this credit card transaction step fool you. Although the word implies accountability in general usage, it carries a specialized technical definition in the payment card industry; authorization only verifies whether or not the transaction amount exceeds the cardholder account’s credit limit, and whether or not the cardholder has reported the card lost or stolen. It makes no further assessment of the transaction’s legitimacy. Once a transaction passes this simple automated test, the merchant assumes full financial liability in capturing the funds. If the merchant mistakenly assumes it is safe to capture funds simply because the transaction has been authorized, the authorization actually endangers, rather than protects, the merchant in the event of fraud.

You are subject to chargebacks.

Issuers sometimes refine their authorization parameters to block requests with suspicious elements, but they do not have the manpower to perform intelligent, detailed analyses of every transaction they authorize. If an issuer happens to authorize a fraudulent transaction and the merchant fails to detect it and captures the funds, the cardholder inevitably disputes the charge with the issuer; the issuer in turn reimburses the cardholder by debiting the processor. Since the processor also has limited resources with which to analyze all of the transactions it funds, it debits the merchant for reimbursement and assesses a standard chargeback fee (specified in the service contract) for the inconvenience. In most cases, the processor also provides the merchant an opportunity to reverse the chargeback, but it is almost always too late for the merchant to present a compelling reason to do so. Inexperienced merchants often plead ignorance when confronted with a chargeback, but it never helps their case; they have failed to live up to their responsibilities and the cardholder remains defrauded because of it. Far more often than not, the merchant loses the transaction amount, the fee amount, and the merchandise.

Chargebacks can impact more than your inventory levels and short-term revenue.

When a cardholder disputes a transaction, the issuer debits the processor before the processor has an opportunity to debit the merchant. This means that if the processor receives a chargeback that exceeds the amount available in the merchant's account, the processor is at risk of financial loss. Remember that processors know only how much money they have deposited into their merchants' accounts; they cannot view account balances or prevent merchants from withdrawing funds. To protect themselves, therefore, processors reserve the right to impose unannounced, non-negotiable emergency funding conditions on their merchants' transactions.

If a cardholder disputes an unrecognized transaction that you captured, your processor may assume that you either do not fully understand your obligation to prevent fraud, or that you are not sufficiently diligent in meeting it. Consequently, your processor may fear that you have accepted additional fraudulent transactions that will inevitably be charged back as soon as the cardholders notice. If your account does not contain enough funds to reimburse all cardholders you helped defraud (unwittingly or not), your capture activity represents a serious financial risk to your processor. To limit exposure, therefore, your processor may hold some or all of your transaction funds aside for a period of time in an inaccessible "reserve account" with no regard for your operating capital needs. This may seem like an unfriendly practice, but it is necessary for any processor that wishes to remain financially solvent, as fraud losses can easily reach thousands or even tens of thousands of dollars for a single ecommerce merchant.

Since issuers provide cardholders up to six months to dispute charges, your processor can leave a reserve account in place for up to six months after your most recent transaction. In the event that your account does not contain enough money to fund all chargebacks issued, your processor will assess a non-sufficient funds fee (also specified in your service agreement) for the inconvenience of having to reimburse the issuer on your behalf. And if your processor is unable to collect on your debt, not only will it refuse to offer you future service, it may also submit your personal details to a fraud control database accessible by all responsible processors. As a result, you will end up blacklisted from processing credit cards through any responsible provider, even if you were an unwitting accomplice in the matter. In other words, lack of information about fraud can cost you the privilege of accepting credit card payments altogether, and this can potentially put you out of business.

There are methods you can use to help significantly minimize your risk.

The only foolproof way to prevent all fraudulent credit card activity on your website is to refuse to accept credit card payments outright. If you take this step, however, you will have difficulty attracting customers away from competitors who offer the option, as it enhances customer convenience and the appearance of legitimacy. Fortunately, you can drastically reduce your risk level by following the guidelines below. Note that most of the effective fraud prevention methods available to you require order analysis prior to funds capture.

1. Use the 'Authorize at Sale, Capture at Shipping' gateway setting in your admin area (under 'Settings' > 'Payment').

While the setting itself does not prevent purchasers from placing fraudulent orders, it provides you the best opportunity to catch them before you become subject to chargeback. It is, therefore, the default (and recommended) setting for all Volusion stores. 'Authorize and Capture at Sale' is not recommended because it does not permit order analysis prior to funds capture, and 'I'll Do Everything at Shipping' is not recommended because it does not permit processing of the CVV2 value (see #3 below).

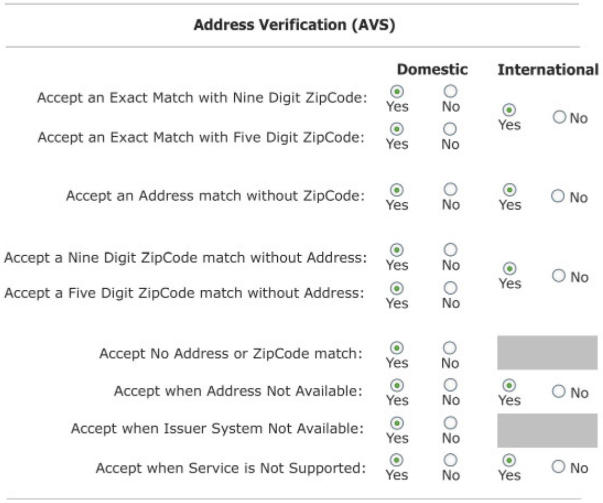
2. Always examine AVS responses.

On all authorization attempts, the Address Verification System compares the numeric billing address variables entered during checkout to the ones stored by the issuer in the cardholder profile. The protection provided by this system is limited because few non-US issuers participate, and because the method can only validate the zip code and/or the numeric portion of the street address; but you can always use these responses to determine a baseline legitimacy level for each transaction prior to funds capture.

On your order details pages, you can find the 'AVS' field located just below the payment date in the 'Payment Log' section. This field displays a single letter, which corresponds to a specific classification that you can reference with your gateway provider. Merchants using Skipjack can do so on the Skipjack website; merchants using Authorize.net can do so on the Authorize.net website.

You can also view AVS responses in your gateway console itself. If you use Skipjack, you can find them in your account (https://secure.skipjack.com > 'View Register') by clicking the cardholder name. The 'AVS' field is located below the shipping address data. If you use Authorize.net, you can find AVS responses in your account (https://secure.authorize.net > 'Transaction Detail') by clicking the transaction ID. The pertinent information is listed under the 'Authorization Information' section, in the 'Address Verification Status' field.

If you process a large enough volume of transactions to render individual order inspection impractical, you can set Authorize.net's AVS filter settings to automatically decline transactions that fail to meet specific criteria at 'Settings' > 'Address Verification Service'. You can change Skipjack's AVS filter settings by requesting specific desired changes in a ticket submitted from http://my.volusion.com to the 'Merchant Services Support' category. Below are the default values:



Address Verification (AVS)

	Domestic		International	
Accept an Exact Match with Nine Digit ZipCode:	● Yes	○ No	● Yes	○ No
Accept an Exact Match with Five Digit ZipCode:	● Yes	○ No		
Accept an Address match without ZipCode:	● Yes	○ No	● Yes	○ No
Accept a Nine Digit ZipCode match without Address:	● Yes	○ No	● Yes	○ No
Accept a Five Digit ZipCode match without Address:	● Yes	○ No		
Accept No Address or ZipCode match:	● Yes	○ No		
Accept when Address Not Available:	● Yes	○ No	● Yes	○ No
Accept when Issuer System Not Available:	● Yes	○ No		
Accept when Service is Not Supported:	● Yes	○ No	● Yes	○ No

If you find the transaction status discrepancy between issuer and gateway to be an undesirable byproduct of adjusting the filter settings, keep in mind that the Volusion software allows you to easily void (via Payment Log command) any authorization you do not wish to capture. You can also do so from your gateway console. In Authorize.net, you can void authorizations at 'Search' > 'Unsettled Transactions' by clicking the transaction ID, then the 'Void' button. The Skipjack Transaction Register provides a 'Delete' option for this purpose in both the list view and the transaction detail view (never execute this option on captured transactions).

3. Collect the CVV2 at checkout, and examine the response code.

The CVV2 is Visa's name for a 3-digit security code printed on the back of the card. MasterCard calls it the CVC2, and Discover and American Express call it the CID (on American Express cards, it is a 4-digit number printed on the face). Since this data is not embossed on the card or stored in its magnetic stripe, it cannot be stolen through many methods used to steal other crucial details that are, such as the card number, the expiration date, and the cardholder name. Therefore, when the purchaser uses the correct security code, name. Therefore, when the purchaser uses the correct security code, the likelihood that they are in possession of the physical card is much greater. This in turn significantly reduces the level of risk associated with capturing the funds. For instructions on enabling CVV2 capture at checkout, see this Volusion support article.

You can find the issuer response code in the 'CVV2' field just below the 'AVS' field in the 'Payment Log' section of your order details pages. As with AVS response codes, merchants using Skipjack can reference CVV2 responses on the Skipjack website merchants using Authorize.net can reference them on the Authorize.net website.

If viewing your Skipjack Transaction Register, you can find CVV2 responses by clicking the cardholder name. The field is located at the bottom of the 'transaction detail' section. Note that if you use Skipjack and require the CVV2 at checkout, American Express transactions will decline unless you submit a ticket from http://my.volusion.com to the 'Merchant Services Support' category requesting that Skipjack also require the CVV2 code.

If viewing the Authorize.net Transaction Detail page, you can find CVV2 responses by clicking the transaction ID; look under the 'Authorization Information' section for the 'Card Code Status' field.

4. Always examine the billing address prior to shipment, even when the AVS response indicates no sign of fraud.

Since only the numeric portion of the street address is required to pass the first part of an AVS check, creative fraudsters can fill out the shopping cart checkout fields with abnormal address formatting that fools the AVS check with the correct numbers, but encourages you to ship to an unrelated address. Also, watch out for fake/generic-looking addresses, such as "1234 Main Street." Although thieves may not be able to receive the ordered merchandise at such addresses, they may simply be using your store as a testing ground for a stolen credit card number. While you may ultimately recover your merchandise in

Examining AVS Responses

Accept when Address Not Available:

This filter refers to occasions when the issuer's system is operational, but it contains no address data for the card used.

Accept when Issuer System Not Available:

This filter refers to occasions when the issuer's system is not operational at the time of the authorization attempt.

Accept when Service is Not Supported:

This filter refers to occasions when the issuer does not participate in the Address Verification System.

Adjusting these settings in either Authorize.net or Skipjack is recommended only as a last resort, because issuers never decline transactions based on AVS responses. This means that when your gateway automatically declines a transaction based on the filter settings, the cardholder account's credit limit is still temporarily reduced in the amount of the transaction. As a result, cardholders may accuse you of having charged their cards when you have not.

these cases, you will not recover the shipping cost, the processor's chargeback fee, or the time you wasted.

5. Be especially careful with orders requesting shipment to a different location than the billing address.

Although there is nothing inherently suspicious about such orders (since gifts are often purchased this way), this is the easiest way for a fraudster to use a stolen credit card to receive merchandise. If you perform no order analysis prior to capture and shipment, you could be making a fraudster's day by sending your merchandise directly to him or her with no strings attached. And even if you verify AVS & CVV2 matches before shipment, paid mail forwarding services essentially allow fraudsters to hire legitimate but unwitting delivery middlemen. If you fulfill the order simply because you know the cardholder's real address, you could be sending your merchandise on its first leg of a journey to a fraudster.

If the shipping contact name is the same as the billing contact name but the addresses are different, you can protect yourself by requiring use of a signature confirmation delivery method. Be sure to avoid "indirect signature" methods, however, which allow anyone at the location or at adjacent locations, even underage persons, to sign for the delivery. Your copy of the signature slip will not serve as a safety net in the event of chargeback unless it contains the actual cardholder's signature. Also, be certain that your chosen delivery method does not allow use of a stored signature from a previous delivery, even if it is the cardholder's, as it will not serve as proof that the cardholder accepted the delivery in question. Finally, keep in mind that AVS does not verify the cardholder name. To be certain that the correct cardholder name has been included on the order, further research is necessary (see #8 below).

If the shipping contact name is different than the billing contact name, signature confirmation cannot protect you. You can require these purchasers to pay by money order, cashier's check, or wire transfer prior to shipment, but you run the risk of losing sales in doing so. Further order analysis is recommended (read on for details).

6. Call the phone number provided with the billing address.

Since thieves can still pose as legitimate cardholders over the phone, this method is not guaranteed to unmask them, but non-working numbers, non-answers, and suspicious conversations with thieves who are not so bold and competent when confronted can help you rule out orders that have raised fraud suspicion for other reasons.

7. Perform a reverse lookup on the phone number or the billing address.

Visit the White Pages website to verify the connection between the phone number and street address provided on the order. This can be especially useful when AVS verifies the address, but you have other grounds for suspicion. A mismatch cannot confirm fraud (the phone number may be that of a cell phone, or simply unlisted), but a match can reduce the likelihood of fraud.

8. Request that the issuer make a courtesy call to the cardholder to confirm the order.

If you are able to obtain the full card number by calling the billing phone number and you are still not certain you have spoken to the true cardholder, Discover (800-347-2000) and American Express (800-528-5200) can call the cardholder at the number stored in the account profile to confirm order legitimacy. Be prepared to provide your merchant number as identification (Discover numbers are 15 digits, American Express numbers are 10 digits). You can also call Visa (800-847-2750) and MasterCard (800-622-7747) to obtain the issuing bank's phone number for this purpose. This may be an attractive alternative to outright refusal to ship to an address when it does not match the billing address.

9. Be certain the customer's IP (Internet Protocol) address and ISP (Internet Service Provider) are in reasonable proximity to the billing address.

You can check this by clicking the IP address above the address information on the order details page. If the billing address is in Los Angeles, for example, but the order was placed from an IP address originating in Indonesia, do not capture the funds or ship the product. When performing this sort of analysis, keep in mind that while an unreasonable IP/ISP combination can confirm fraud, a reasonable IP/ISP combination cannot rule it out, as determining IP location is not an exact science, and it is also possible to spoof one.

10. Be wary of all international orders, especially ones from high-risk regions like Southeast Asia, the Middle East, Africa, Eastern Europe, and Central America.

Many countries in these regions are hotbeds of credit card fraud. Since they are unlikely to ever supply you a legitimate sale, orders from them may not even be worth the hassle of reviewing.

11. Watch for multiple failed order attempts from the same purchaser.

While many consumers do regularly use two or three cards (and do not keep close track of the cards' spending limits), be cautious when you see multiple attempts in which certain variables remain consistent while others change, such as a consistent IP address with different customer names, or a consistent credit card with different billing addresses.

12. Use your IP Firewall to block fraudsters from repeat attempts.

If you catch someone trying to defraud you once, this admin area tool can make it more difficult for them to access your store again in the future. For instructions, see this Volusion support article (note that it is possible to block whole IP ranges of problematic regions).

13. Be wary of email addresses that contain random-looking character sequences, especially addresses provided through free services like Yahoo, Gmail, or Hotmail.

These accounts are relatively quick and easy to create and require no identity validation. Anyone trying to scam merchants can create one or more of them to avoid having to use their own legitimate personal email address on fraudulent orders. Since millions of people use these services, however, it can be difficult to generate a logical choice of address that is not already in use. This restriction is actually helpful for merchants who perform thorough order examinations because most people looking to create a mail account to use in a legitimate fashion will take the time to find a sensible choice of address, whereas people looking to create an account for unscrupulous purposes may feel that the quickest and easiest way to find an unused address is to randomly mash the keys to generate part (or all) of it.

14. Be wary of any order placed with an email address that includes a different name than the cardholder's.

If the cardholder is "Brian Smith," for example, and the email address is "jerry_williams86@gmail.com," ask yourself why "Jerry" is using Brian's card, or why Brian is using Jerry's email address. As described above, it is quite simple for thieves to create fake (but legitimate-looking) addresses to help maintain their anonymity. While they may take the time to create an address that looks legitimate enough to pass as the actual cardholder's, it is often quicker and easier to use an account generated previously; in these cases, no apparent connection will exist between the cardholder name and the email address. For this reason, email addresses that include names that match the cardholder's name are less likely to be fraudulent, since setting up the accompanying email account requires extra labor that is not necessary for success. Remember, however, that verifying legitimacy of the cardholder name requires research of its own. Never assume the billing contact name is legitimate.

15. Be wary of suspicious-looking customer names.

Fraudsters often take care to use the true cardholder's name on fraudulent orders to enhance the thoroughness of the deception, but since the correct cardholder name cannot be verified at a glance and is not required for a successful authorization, they may also take a shortcut and use a false name instead. Fortunately for you, these names often look just like what they are.

16. Be wary of atypically-high transaction totals.

If your average sale is $30 and you receive an order totaling over $1000, it may seem too good to be true because it probably is. A large volume order of your highest ticket items may make your mouth water, but this is the riskiest type of order to fulfill, and you should treat it with appropriate skepticism; if the transaction is not legitimate, you stand to lose as much as you hoped to gain (and more).

17. Take advantage of Volusion's Fraud Score service.

For a low monthly fee, you can receive the benefit of automated examination of many of the factors outlined above, as well as of general worldwide purchasing trends and a vast database of past transactions. Each examined transaction displays a numerical score directly on the order details page that serves as an at-a-glance indication of the general risk level associated with funds capture. The service also provides a clickable itemized breakdown of safe and risky transaction elements to help you pinpoint potential problem spots. To review purchasing options, log in at http://my.volusion.com, click 'Manage plans / orders', and click 'ADD' next to the 'Fraud Score' listing.

18. Most importantly, Use common sense.

If something about an order does not look or feel right, do not capture the funds or ship the merchandise. If you have any reason to suspect fraud and the merchandise is too valuable for you to lose outright, hang onto it for a better selling opportunity in the future. In this industry, merchants have to look out for themselves. When your liability is high, it is usually better to be safe than sorry. All successful issuers and processors use this philosophy, and so should all merchants who wish to succeed in ecommerce.

Now that you are familiar with the methods credit card fraudsters use to exploit merchants, you understand your processing liability, and you are aware of best practices to follow to protect yourself, you can focus on running a safe and profitable online business.