Fraud Detection Services for Card-Not-Present Transactions
NC Office of the State Controller

For "card-not-present" transactions, signatures are not obtained and the track data cannot be captured, increasing the risk of potential chargebacks. Three fraud detection services are available through the merchant card networks which merchants can choose to subscribe:

1) Address Verification Service (AVS); and/or
2) Security Code Verification Service (CVV2/CVC2/CID); and/or
3) Cardholder Authentication Service

All card networks use the term AVS when referring to "address verification service." In the case of "security code verification service," different terms are used by the card networks: Visa refers to CVV2; MasterCard refers to CVC2; while American Express and Discover both refer to CID (Card Identification Data).

In the case of "cardholder authentication service," two programs offered are "Verified by Visa" and "MasterCard® SecureCode™." The services offered by Visa and MasterCard involve the cardholder having to enter a password in order to verify their identity, and only applies to cardholders that have subscribed to the optional service with their card issuing bank. The Visa and MasterCard cardholder authentication services are not widely utilized by merchants. As an alternative, merchants accepting payments via their website should consider developing their own method of authenticating a cardholder. For example, a merchant could require the cardholder to enter some type of identification number, such as student number or invoice number before being able to make a card payment.

SunTrust Merchant Services (STMS) accommodates all of the fraud detection services for card-not-present transactions, but does require any of them. However, merchants participating in the Discover Network Card contract should be aware that Discover requires AVS services to be utilized for all card-not-present transactions (both numeric billing street address and zip code), or be charged an additional fee if not used. The fee charged for not capturing the required AVS data is $.50 per transaction. For Discover, the CID service is optional.

Not all vendors' credit card capture applications are capable of accommodating the fraud detection services, and not all applications work the same. Each system can normally be "configured" in a variety of ways, depending upon the merchant's level of fraud protection it desires to have in place for "card-not-present" transactions.

Fraud Schemes

Using at least one of the fraud detection services obviously helps to prevent fraud against the merchant. However, it also helps to prevent the merchant's website from being used by individuals that have possession of stolen card numbers to involve the merchant in a scheme to validate whether a stolen card number is valid or not. The scheme involves individuals making payments at a merchant's website with a stolen card number, not for the purpose of securing a product or service, but to use the website's authorization process. Such payments are normally for small amounts. If the card is accepted on the merchant's website, the individual will then use the card elsewhere, for larger purchases. Websites that accept variable payments, or those that accept donations (e.g., non-profits), are highly susceptible to this scheme.

There are several implications for the merchant in such a scheme. The merchant will likely have to deal with a chargeback when the cardholder determines the payment was associated with a stolen card number. For each chargeback, the merchant is levied a $9.75 service fee by STMS. A merchant with a higher-than-acceptable number chargebacks is subject to termination of its services from STMS.

Merchants should monitor payments made on its website to detect suspicious payments, as well as payments for amounts that are not typical. Once a website is targeted and the fraudulent payments go undetected, the number of such fraudulent payments normally increases, and the website is made known to other schemers, normally from foreign countries.

Address Verification Service (AVS)

There are normally several levels of AVS that can be selected. When AVS is utilized, there is a "response code" received whenever the authorization process is performed. Below are examples of some of the response codes that could be received from the merchant card processor:

General AVS Validation Codes	
B	Address information not available in transaction information, so AVS check could not be performed
E	An error occurred on the processing network during the AVS check
G	The credit card issuing bank is of non-U.S. origin and does not support AVS checks
R	AVS was currently unavailable at the time the transaction was processed. Retry transaction
S	The issuing bank does not support AVS
U	Address information is not available for the customer's credit card

Street Address matches, but 5- or 9- digit ZIP does not	
Y	The street address and the first 5 digits of the ZIP code match perfectly
A	Address matches, but ZIP code does not

Street Address does not match	
W	The 9-digit ZIP code matches, but the street address does not match
Z	The first 5 digits of the ZIP code matches, but the street address does not match
N	Neither the street address nor the ZIP code matches the address and the ZIP code on file for the card

The vendor's system can normally be configured to handle each AVS response code in accordance with "rules" that may be established. For example:

- A high level of verification is to accept only Street Address and Zip Code matches
- A lower level of verification is only Street Address matches (numeric not alpha matches)
- An even lower level of verification is only Zip Code matches (5 digits)

With many possible reasons why an address and ZIP code may not match, merchants should carefully consider their business's level of risk when configuring its AVS mismatch rejection settings. For example, multiple numeric values in the street address field must be in the correct order. Cards issued by non-US banks generally do not have zip codes and are subject to being rejected.

Security Code Verification
Card Verification Value Service is another option that capture applications offer to detect fraud for card-not-present transactions. Visa refers to this as CVV2, MasterCard as CVC2, and American Express and Discover s CID. The following table shows typical CVV2 "response codes" that could be received.

Card Verification Value (CVV2) Response Codes	
Code	**Value Description**
M	CVV2 Match
N	CVV2 No Match
P	Not Processed
S	Issuer indicates that CVV2 data should be present on the card, but the merchant has indicated data is not present on the card
U	Issuer has not certified for CVV2 or Issuer has not provided Visa with the CVV2 encryption keys
Empty	Transaction failed because wrong CVV2 number was entered or no CVV2 number was entered

Just as in the case of Address Verification Service (AVS), a vendor's system can be configured to reject a presented card transaction if there is no security code match.

The AVS response code and the security code response should not be confused with the "authorization code" that may be received. The authorization code applies to validity of the card and the funds availability, while AVS and CVV2/CVC2/CID pertain to fraud detection.

Merchants should be aware that AVS and security code services are tools to assist in detecting fraud. They are not "guarantee services," as chargebacks can still be experienced. Any authorization that is approved is subject to chargeback at a later date.

Funds Encumbrance Implications
If a merchant utilizes AVS and/or CVV2/CVC2/CID verifications, and its configuration rules specify certain codes to be rejected, the system rejects the transaction based on the AVS or security response code. However, the authorization code may be valid, which is what causes the cardholder's funds to be encumbered.

There are at least three ways funds can become unencumbered: 1) Some vendors' systems will automatically resubmit a transaction to the card processor to effect a release of the encumbered funds; 2) Funds will become unencumbered (drop off) after a certain number of days, if the merchant does not follow up on the authorization by sending the batched transaction to be settled. The drop off time is determined by the cardholder's bank and ranges from 24 hours up to seven days; 3) The merchant can call the card processor or issuing bank and authorize a release of the encumbrance.

The funds encumbrance situation can cause customer relations issues with the cardholder. The cardholder may incorrectly have the impression that the merchant has charged his account, while it is his bank that has placed a "hold" on the funds. Also, a subsequent correctly presented

transaction could be rejected if a previously rejected transaction caused the cardholder's credit limit to be reached. However, the cause of the rejection is normally the result of the information that the cardholder presented, not something the merchant did wrong.

The encumbrance of funds is a standard industry practice. For example, when a card is swiped at a gas pump, the card is typically encumbered for $75, even though only $30 of gas may be purchased. This is because the gas pump does not know how much gas is going to be purchased at the time the card is swiped. Similar holds apply with hotel reservations and auto rentals, etc. The funds are not unencumbered until the batch transaction containing the actual amount is transmitted to the card processor, some days later. The initiation of large dollar transactions obviously has a greater effect on the availability of funds associated with the cardholder's credit limit.

If a merchant has a low factor of risk associated with Internet initiated transactions, it may consider being lenient in its application of AVS and security code services. This is especially the case if the card transaction is for a service that can be canceled. Conversely, if it has a high frequency of suspicious transaction activity, or if it incurs abnormally high discount rate charges, AVS may be an appropriate method of protection. Such fraud detection services are more commonly used in online shopping environments. Merchants accepting the Discover Network Card should consider Discover's requirement that AVS for both the street number and zip code are required in order to avoid an additional fee of $.50 per transaction.

Should a merchant subscribe to the security code service, it must adhere to the PCI Data Security Standard requirements and associated card associations' rules regarding not storing the security code (considered track 2 data) subsequent to initiating the authorization. Fines range from $50,000 for level 2 merchants, to $100,000 for level 1 merchants.

All state agencies should adhere to the E-Commerce policy issued by the Office of the State Controller entitled, "Authorization for Merchant Card Transactions." The policy states in part: "*Each participant shall be responsible for developing and documenting procedures to handle merchant card exceptions. The procedures shall include the handling of transactions for which an approval is denied, unauthorized card use, non-match of address verification, the use of an alternative payment if authorization is denied, and charge backs."* The policy can be viewed in its entirety at:
http://www.osc.nc.gov/Credit_Card/AuthorizationforMerchantCardTransactions.pdf

For those agencies utilizing the state's Common Payment Service (CPS), both AVS and security code response codes are accommodated. SunTrust Merchant Service (STMS) may levy an additional $.02 per transaction fee for transactions involving AVS.

Each agency should make its own evaluation of the types and levels of fraud detection services it may subscribe to, and authentication techniques it may deploy. Consultation should be made with the vendor that provides the card capture application.