TELEPHONE SCAMS

These calls normally originate from overseas and the caller typically requests that the merchandise be sent to a location outside the U.S. The purchase is made with either a stolen credit card and/or credit card number. This scam targets retailers in all markets (including hardware) throughout the country.

Committing to the sale of product to someone you can't see, don't know and have never met, over the telephone who wants the product mailed to a non-local address and uses a credit card for the purchase is extremely risky. Many Ace retailers have become victims of this international theft scam – and the fact that the credit card is stolen usually does not become evident until days later. West Africa has been the primary source locale for these scams, but they can originate anywhere.

There are actually two variants of this scam.

SPRINT RELAY SERVICE

This scam uses the Sprint Relay Service (***www.sprintrelayonline.com***) to place orders with stolen credit cards. A relay service places phone calls for people who are hearing impaired, but scammers take advantage and use the Internet relay because all calls are free, including long distance. Ace retailers have been contacted requesting purchases of items such as high-end locks, power tools, paint etc. Then they are requested to ship the merchandise to Africa, Nigeria, Ghana and other such locations. Some retailers have taken these credit card orders and actually sent the merchandise, to only find out a few later that they have been scammed and have no way to recoup their losses. Others have become suspicious and questioned the caller about why they would want to pay for shipping fees when they most likely could purchase the merchandise locally for less.

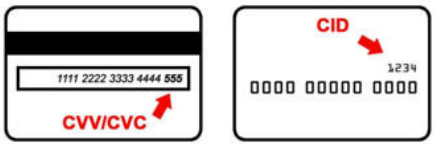
WEST AFRICAN RE-SHIPPERS

This rapidly expanding scheme often originates in West Africa, but can originate from other locations as well. A typical scenario includes callers, using stolen or fraudulent credit cards, requesting to purchase high ticket items for shipment to a domestic address. This is done to allay concerns regarding suspicious international shipping orders. An expansive network of *re-shippers* continues to be recruited and used by the perpetrators of these schemes. Recruitment is done via Internet Relay Chat (IRC) rooms, web-based job postings and even telephone solicitations. In return for the use of their residence or business address, the recruited re-shipper is often allowed to keep certain merchandise as payment, or is paid with counterfeit cashier's checks.

PREVENTIVE MEASURES

- Simply do not accept these type transactions.
- Make it a policy not to accept international phone orders, period.
- If you decide to proceed with the order, then you should do four things first –
    - Ask the caller for the card's CVV/CVC/CID number (for Visa, MasterCard, and Discover cards, the CVV/CVC numbers are on the back of the card (the last three digits of the string of numbers below the magnetic strip). For an American Express card, the

CID four-digit number is on front of the card) NOTE: If the actual card has been stolen, the thief would be able to supply this number. If the caller indicates that, for whatever reason, he is unable to supply the number, this would be a huge red flag that the card number has been stolen or is otherwise bogus.



- Tell the caller that before processing the transaction and shipping the merchandise, you will have to verify the credit card, and for him to call you back in an hour. If he hangs up on you, or if you do not receive a call back, take that as confirmation that the caller was attempting to scam you.

- Use the "Address Verification Service" (AVS) offered by all credit card companies to verify the cardholder's billing address. This service was designed specifically to assist in minimizing the risks of being victimized by these types of schemes. Using AVS allows a merchant to verify the cardholder's billing address with the card issuer, either telephonically prior to the sale, or electronically during the actual sale at the same time the authorization is requested. The card issuer compares the address provided by the merchant to the billing address it has for that customer's account and replies with a code indicating the results of that comparison (i.e., exact match on both the street address and the zip code; no match on either; or a partial match on either the street address or the zip code). This additional information helps retailers make more informed decisions about whether to complete a transaction or take an additional action to protect themselves. Go to **http://www.emsecommerce.net/avs_cvv2_response_codes.htm** for a listing and explanation of the various AVS and CVV2 response codes.
- Request the CVV/CVC/CID information from the back of the credit card and confirm the match. This can normally be done at the same time you use the AVS.

MAJOR CREDIT CARD CONTACT NUMBERS FOR AVS VERIFICATION:

- **Visa/MasterCard** - 800-944-1111, Option 2
- **Discover** - 800-347-1111, Option 2
- **American Express** - 800-528-2121, "Tell me my choices" - "Verify Name & Address"

LIABILITY FOR FRAUDULENT INTERNET, MAIL AND TELEPHONE ORDER TRANSACTIONS

Retailers who accept non-face-to-face transactions also accept liability for these transactions in the event they prove to be fraudulent. If the transaction is fraudulent, a chargeback will occur on your bankcard recap.

For information on credit card transaction charges, contact Ace Bankcard at 630-990-6593. You can also go online to **www.acelossprevention.com** for additional prevention measures or contact Retail Loss Prevention at 630-972-2670.