hang up **on fraud!**

evertec®

fraud alert for manual transactions

The safest way to process card payments in your terminal is by using the chip or magnetic strip that authenticates your customer's card. Card-not-present transactions entail a high risk of loss for your business. Therefore, if your business depends on sales by phone, catalog, Internet, pre-authorized orders, or installment sales, your service contract with us establishes the business' responsibilities for the secure management of these manual transactions.

Make sure to review the terms and conditions of your contract with us, so you may learn the requirements and minimize the risk of loss for your business when conducting card-not-present transactions. Stay alert for these signs that may indicate card-not-present fraud to protect your business and follow the recommendations described here to decrease the possibility of falling victim to a fraud.

fraud scheme signs

- The customer places orders that are larger than what is normal in your business.
- The customer includes large amounts of the same item or very expensive items in the order.
- The customer requests "urgent" or "next day" shipping.
- The customer requests that the order is shipped to an international address.
- The orders are sent to the same address and bought with different cards.
- The customer uses an email from a free email service (Yahoo, Gmail, etc.) instead of having their own domain.
- The customer requests that you charge the transactions to several card numbers that are sequential.
- The customer provides several card numbers, and some transactions are declined.
- The customer charges multiple transactions to a card during a very short period.
- The customer could ask the business to pay the merchandise shipment, by wire transfer, to a shipping company chosen by the customer.
- Once the business completes the wire transfer, the customer may request that the merchandise shipment be stopped to include additional orders since their partners have become interested in acquiring additional merchandise.
- The customer asks to include the shipping cost in the total sum of the transaction.

recommendations

1. Use AVS.

This is an address verification service provided by Evertec that validates the zip code specified in the cardholder's billing address, as registered in the issuing bank. AVS only verifies addresses within the U.S. To request this service, send us an email to merchantclaims@popularmerchant.com, include your Merchant ID, Terminal ID and indicate you want to add the zip code validation.

2. Request the CVV number.

For an additional level of security, verify the card's authenticity by asking for the credit card's three-digit verification code. Depending on the issuer, it may have different names like CVV, CVC, or CID. This code is often missing in stolen/fraudulent cards or is not available, as is the case for compromised card numbers or generated account numbers.

3. Validate the card's expiration date.

4. Validate the customer's physical and mailing address.

As an alternative, before sending the order to the customer, confirm the order through the billing address, not the mailing address.

5. Only send the merchandise to the cardholder's billing address.

You may want to request a certified signature as proof of delivery of the merchandise.

6. Check online

the existence of the business and the person making the purchase.

7. Ask the customer for additional information,

such as a phone number that is reachable both day and night. Call them later to confirm the sale.

8. Ask for the name of the bank found on the front of the card

and the bank's customer service number found on the back of the card. Search on Google for the BIN number (first four digits on the card) and confirm if the card corresponds to the same issuing bank.

9. Deactivate the Manual Access functionality.

If necessary, the functionality can be deactivated. If you want to deactivate it, send us an email to merchantclaims@popularmerchant.com please include your Merchant ID, Terminal ID and indicate that you want to disable the Manual Access functionality.

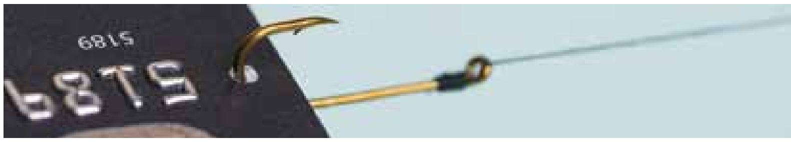
10. If you want to keep the Manual Access functionality activated,

make sure that the password remains confidential. Only share the manual access password with trusted personnel. If you share the password with other employees for specific situations, change the password as soon as possible and keep it private. By sharing the password, you are responsible for any possible loss that your business may have.

fraud alert for refunds

Unauthorized refunds represent a loss for your business. By entering the authorization code, the employee is authenticating, on behalf of your business, that the transaction complies with the business return policy. If your business has a return policy, your service contract with us establishes the business' responsibilities for the secure management of these transactions. Make sure to review the terms and conditions of your contract with us, so you may learn the requirements and minimize the risk of loss for your business. Stay alert for refund fraud so you can protect your business.

Refunds should only be processed if there was a previous sale, and the refund amount should not be greater than the original sale. The amount must be refunded to the same card used for the original sale. Once the refund is completed, it cannot be recovered. Therefore, the money reimbursed to your customer cannot be returned to the business and the business automatically loses the money.



fraud scheme 1

Employees who are authorized to process legitimate refunds from your customers, process the refunds to their personal cards and/or to the cards of family members and/or friends.

recommendations

- Be alert of the behavior and patterns of your employees.
- Do not share the password. If you need to share the password, only do so with trusted personnel. If you share the password with other employees for specific situations, change the password as soon as possible and keep it private. By sharing the password, you are responsible for any possible loss that your business may have.
- If your business does not accept returns and your refund feature is enabled, contact us to disable it at merchantclaims@popularmerchant.com please include your Merchant ID, Terminal ID and indicate that you want to disable the Refund functionality.
- Remember that an entry error in the terminal can be voided. If you have questions on how to do the reverse, contact our service center at 787-751-1401. The ATH transactions cannot be voided because the transaction is instantaneous, different from credit card transactions. If the transaction was already processed in the deposit (Settlement) send us an email to merchantclaims@popularmerchant.com please include your Merchant ID, Terminal ID, Sales Slip, and indicate whether the return is partial or total (instruction to perform).

fraud scheme 2

Scammers call asking for a reimbursement payment claiming that it was authorized by the management or the person in charge of the business. This type of fraud can cause losses for your business if you do not stop it on time.

- Scammers call your business claiming that they work for a government agency, a consumer protection group, a law firm, a shipping company, a charity, or some other organization. They can also communicate by mail, email, web pages, text messages, or social media.

- Scammers claim that the business must make a payment to keep a license or contract in effect, receive merchandise, or solve other urgent situations. They may claim they are in communication with your business' management regarding this situation to try to legitimize the call.

- Scammers can ask the employee to make a refund to their personal debit/credit card as a way to supposedly get their money back and then use those funds to make a money transfer through Western Union, MoneyGram, or another money transfer company.

recommendations

- Keep your employees informed about these fraud schemes. Scammers will make them feel like they can be trusted.

- Government agencies and legitimate organizations will not ask for money using your employees' personal cards or money transfer services.

- Question any action with a false sense of urgency, especially when it happens outside of business hours.

- Inquire about any organization or government agency that communicates with you or with one of your employees. For government agencies, search for the agency number on your own and call them to confirm if they reached out to you. Do not call the number you were given by the person who called you. For organizations or businesses, search the name on the Internet along with words such as "complaint," "scam," or "review."

- Never process refunds without a previous purchase and especially not to their personal cards.

- Verify the veracity of the reimbursement request directly with the management or the person in charge before making the transaction.

If you suspect that you have fallen victim to these fraud schemes, contact the police immediately to file a complaint and contact your bank or financial institution.

evertec®

the technology **of the possible**