JHJ Jewelers Crime Alert Network

Aleah Arundale · ·

HELPUL POST FROM LEO
HAVE ALL EMPLOYEES READ THIS
FORCED OR OFF-LINE CREDIT CARD TRANSACTION SCAM
1. Make Sure ALL Employees see this
2. If you don't get a clean chip read, you are at risk
3. If you manually Enter a Credit Card, you have NO RECOURSE on a Chargeback
4. Never Ever take the customers phone to "talk to their bank"
5. Never let anyone other than your own processor walk you through some abnormal procedure on your credit card terminal
6. A Forced transaction can only be activated via your terminal, and the bad guys know how to do this.
7. Just seeing an ID to match the card will not save you
8. YOU HAVE TO GET A CLEAN CHIP READ, to have the best chance.
9. Any phone order is risky as you don't have the card in hand, again pictures of ID will NOT save you from a charge back
How it works, The MF comes in to make a purchase (Usually BIG), card may get declined at first or you can't get good chip read. The MF may act like they are on the phone with their bank to "let them know" they are making a purchase at your store. They will often put you on the phone with "the bank". Never take their phone to talk to "their" bank. NOTE: never ever accept this, they will have an accomplice act like the bank. They will walk you through a forced or off-line transaction, where you key in the info, or even swipe the info (Magnetic or even chip read). BUT they had you go into the menu on your credit card terminal to BYPASS your merchant processor. You can enter any authorization number as it is not even being looked at or processed by your processor – hence the name forced or off-line transaction. You can use the authorization "666", the mark of the devil, it will go through. Then a few weeks later and sometimes even months later get notification that you are getting a chargeback. The REAL cardholder did not make the purchase, and you are done.

All reactions:
41Stacey P Horc