For Oklahoma Bankers Association – April 2016 issue
Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services, LLC

Declined Card Override: The Scam

There's a loophole in the debit and credit card authorization process and scammers are making a huge profit from it, at retailers' expense. It's known as the "declined card override scam" or the "forced approval code scam." Despite the fact that this loophole has been exploited for years and caused significant losses to businesses nationwide, it's once again being carried out across the country.

High level, here's how it works:

An individual comes into a retailer location and presents a card (debit or credit) for a purchase. The business runs the card and it declines. The individual then gets on the phone, claiming to call the card issuer. The scam then goes one of two ways, and both are disastrous:

1. The individual says the card issuer said to type in a code to authorize the purchase, that something was merely wrong with the card mag stripe. Once the business enters the provided code, the sale "approves." OR
2. The customer gives the business his/her cell phone, stating his issuing bank is on the phone. The person on the phone, claiming to be from the card issuing bank, gives the business an "authorization code" which, when the business enters, the transaction "approves."

Here's the problem. The individual did not call the issuing bank; the issuing bank did not provide an override code. Since the bank never issued a real authorization, it isn't valid; therefore, the business just took a loss.

While the scam has been around for some time, losses are increasing at alarming rates. In 2014, Investigators say a man was able to make more than $300,000 in fraudulent purchases from Apple stores across the country using this scam, pulling it off successfully at 42 different locations. Also, recently a 29-year-old defrauded Victoria's Secret, Banana Republic, and several other retailers out of $557,690 using the same scam.

The best advice I have to give is to train your front-line staff, the ones who swipe cards for purchases, that they should never accept a phone or "override" code from a customer. If the customer claims there's a "problem with the card, I will call," your staff should be trained what to do instead. I suggest that all retailers call the number on the back of the card personally. If given an "override" or "authorization" code over the phone, have your staff document who they talked to and when as documentation in the case of a chargeback.

About the Author

Rayleen is the CEO of RP Payments Risk Consulting Services, based in Orrick, MO. She travels the country presenting at fraud, payments and security conferences on topics ranging from Mobile, fraud, payments risk management, and information security. Previously she was the Director of Compliance and Fraud at a regional payments association for 8 years, and worked financial crimes investigations for a community bank for 7 years. Rayleen has been writing and presenting for 10 years.