THE VOICE OF FOOD RETAIL

Feeding Families Enriching Lives

POS Credit Card Fraud Escalates Post EMV – Best Practices

Normally the FMI Electronic Payment Systems Committee is full of creative ideas and sure we can tackle anything presented to us. But the latest escalation of chargebacks on credit that our experts put at a 400-1000% increase over 2015 numbers had them stumped.

We reached out to law enforcement, reached out to congressional committees, reached out to the card associations and reached out to asset protection experts. We put the best ideas of the group together and offer the following advice and a web page where we can add additional ideas, suggestions, tips and encouragement to get this problem under control.

The first step is understanding the scope of problems you are experiencing, as there seem to be a couple of different problems. Some of our folks are seeing what we are calling "organized crime." When a card is used 100 times in your store(s) in a couple of days; that is organized crime and clearly there are multiple people involved in this fraud. On the other hand, when one individual uses a card in your store and then tells their credit card company that they were not in the store and did not buy the products, that is still a crime, you are still out the money, but at least for now, it seems to be the work of one person attempting to take advantage of a bad system or bad issuers happy to charge back and ask questions later because of their "zero liability." This term "organized crime" is clearly not based on a legal definition, just recognition that there is clearly more than one type of problem we are seeing simultaneously.

Getting a handle on the problem:

1.) Track your chargeback rates and work to identify where your greatest vulnerabilities are in the store.
2.) Coordinate with local law enforcement and ask for any trends they may see that could be the work of an organized criminal element. Share your experience with them.
3.) Fraudulent transactions are a crime, so ask law enforcement how and when they may suggest you file a police report for chargebacks resulting from fraudulent transactions and any terminology you should use if you believe a particular chargeback may be linked to others.

Putting in-store controls in place:

1.) Gift cards are a prime target for criminals for a number of reasons. A person can buy a high denomination gift card, they are lightweight and easy to transport and they are easily sold on the Internet. Several FMI members have taken steps to mitigate this risk using one or more of these approaches:

a. Moving the card-branded gift cards that can be used in any store, behind customer service.
b. Restricting selling high value gift cards to certain hours of the day (example: 6am-10pm).
c. Only allowing cash, or PIN-enabled debit cards for the purchase of gift cards.
d. Requiring a photo ID for gift card transactions.
e. Removing gift cards from self-checkout lanes.
f. Setting up a point of sale system prompt for managers' approval for gift card transactions above a certain dollar amount.
g. Not allowing purchase of gift cards with a prepaid or reloadable Visa, American Express, MasterCard or Discover card.
h. Limiting the value and/or the number of gift cards that can be purchased in a single transaction or on a single card in a certain period of time.

Looking Beyond Gift Card Fraud to All Credit Transactions

2.) We are seeing fraud now well beyond gift card fraud. You may want to put additional precautions in place for **any** credit card transaction:
   a. If you are testing EMV in-store and have a register running EMV, direct all gift card, high value or questionable transactions through that lane. This could significantly lower your chargeback exposure.
   b. Require a 100% ID check on all credit card transactions, or ID over a certain dollar value or ID on any customer not using a loyalty card. If you can say that you check ID 100% of the time or can link a transaction that was charged back by a customer who presented a loyalty card or is show via camera to be in the store purchasing products at the time of the transaction, your ability to fight a chargeback is greatly enhanced.
   c. Post signage at the POS explaining this fraud and your response to combatting fraud and protecting your customers and your intent to involve law enforcement. The sign alone may be enough to move the criminal to another location. Plus it cuts down on time your cashier has to explain why they are asked for ID and the customer in front of them using a PIN debit card was not asked for ID.

WHY AM I ASKED FOR ID ON CREDIT TRANSACTIONS?
The supermarket industry has seen an extraordinary level of fraud on credit card transactions in the last several months on both chip and magnetic stripe cards. In an effort to keep your information safe and keep our prices low, we are asking for your ID to confirm your identity on a credit card transaction. We are not experiencing fraud with PIN debit or PIN credit, so if you insert a PIN, you will not be asked for ID. We are working closely with law enforcement and are filing police reports when fraudulent transactions occur.

d. Some companies have added address verification system (AVS) to their credit card processing. As frequently seen at gas pumps, it prompts the customer to enter their 5-digit zip code at the point of sale. If they get a mismatch, they have trained all cashiers to ask for ID.
e. Prohibit manual entry if the magnetic stripe does not work or send that transaction to a customer service desk for more scrutiny.
f. Implement CVV verification on manually entered credit transactions or all credit transactions.
g. Require a manager's override on any large order (over $1,000). An order at a grocery store for more than $1,000 (unless you know the customer and the reason for the transaction – hosting a large party/caterer/restaurant owner) should cause immediate concern/scrutiny.
h. Implement ID check and transaction amount limits per customer and per day to help mitigate risk. Members are reporting cards that have been used more than 100 times in stores in 2 days. You need to have a mechanism in place to make sure this type of "organized crime" does not happen to you.

3.) Remain vigilant against any kind of suspicious activity, such as:
a. Guest/customer attempting multiple credit cards with declines.
b. Guest has a stack of credit cards visible and outside of wallet.
c. Pay close attention to cards issued by international banks in Asia and the Middle East, etc.
d. Buying large quantities of open value gift cards.
e. Buying large quantities of beer or wine.
f. When asking for ID, the customer becomes agitated, nervous or in a hurry.

In response to our requests, both Visa and MasterCard have offered more specific information available on our web page.

FMI's EMV Chargeback Page
http://www.fmi.org/emv-credit-chargebacks-best-practices-and-guidance

Bottom line, you are certainly not the only supermarket being defrauded, but be aware, be vigilant, and be prepared and share what you learn.

In considering any actions, you need to consult your contracts and the operating rules of the card associations.