How to Avoid EMV Chargebacks

Steps to help card-present merchants minimize the flood of EMV Chargebacks

More Chargebacks than Expected

Six months after the credit card fraud liability shift, merchants who have not implemented chip card technology are complaining about a larger number of chargebacks than they expected. One payment network reports an increase of 50% in chargebacks for card-present transactions among some 250,000 merchants.[1]

The reasons for the large increase are not clear. Some fear abuse of the chargeback system, but card companies say that the increase is normal and similar to what was experienced in other markets where EMV was introduced.

They note that all EMV chargebacks are new to merchants and urge them to adopt chip technology to avoid the liability. However, some experts worry that smaller merchants who don't want to deal with the chargebacks will give up and desert the payment card system altogether.

Lawsuits and Delays

A few merchants have resorted to suing the networks and issuers, claiming that they were not given enough time and were not warned of the large dollar amounts involved.[2] The card companies counter that merchants have had five years to prepare and they should know the new rules. Industry experts say that card companies are working with merchants to smooth out the bumps in the chargeback system.

Many merchants already have EMV terminals but face delays from processors who are not EMV ready. A shortage of technical expertise is also delaying adoption of the technology. Stricter EMV installation requirements recently adopted by VISA could be adding to the problem.

What you Should Know About EMV Chargebacks

While the industry sorts out EMV, we consider it worthwhile to help merchants avoid as many chargebacks as they can by understanding the EMV chargeback landscape.

- If you haven't upgraded to EMV terminals, you will be liable for a good portion of the chargebacks that the banks were previously absorbing.
- The liability starts when you swipe a chip card. If there is fraud or a dispute involved, you will be eating it not the bank.

- Even worse is swiping a counterfeit card. You may think that you're off the hook since there's no chip, but there's no way to know on a non-EMV terminal that it should be a chip card. If so, you're still liable.

- You should not be liable for chargebacks on valid cards without a chip, even though some merchants claim to be getting these.

It's interesting to note that the risk of fraud may have increased for those merchants without EMV. Smart criminals will avoid merchants with EMV terminals, making those without them more attractive targets.

Steps to Avoid EMV Chargebacks

Processing transactions correctly at the time of the sale is the most effective way to avoid EMV chargebacks. Here are some best practices:

- Always process chip cards as intended by inserting the card and following the instructions on the terminal.
- Never swipe or key in a chip card. You're not protected if you do.
- If a chip card is declined, do not swipe or override, ask for another form of payment.
- Request a signature and verify.
- Swipe non-chip cards, don't manually enter account numbers.
- If you must manually enter a card, check the expiration date and make an imprint.
- Always check for fraudulent cards – See steps below

The one best thing you can do to avoid chargebacks is to upgrade to EMV chip card terminals, shifting the fraud liability back to the banks. Check with your processor to see if they are ready and can certify proper installation.

VISA now requires that only PCI-certified Qualified Integrator and Resellers (QIR) professionals should be used by Level 4 merchants for the installation of POS terminals, application implementation and integration services. QIR certified professionals have received advanced training to ensure the proper installation and data security of POS systems.

8 Ways to Spot Counterfeit Credit Cards

To avoid unnecessary chargeback liability, make sure that retail employees are well-trained on these ways to spot counterfeit credit cards:

1. The hologram sticker is dull or two-dimensional.
2. A damaged magnetic stripe.
3. The signature strip material is not different than the surrounding plastic.
4. The numbers are misaligned or unevenly spaced.
5. The microprint numbers don't match the card number.
6. The UV Logo is missing under black light (look for AM EX, MC, V, or Discover)
7. The last four numbers printed on the receipt don't match the card.
8. Suspicious behavior, rushing, creating distractions or nervousness.

A Proactive Approach

As the industry moves forward with EMV adoption, merchants who take a proactive approach to avoiding chargebacks, whether or not they are EMV ready, will be in the best position to benefit from the technology change. Proper implementation of EMV technology is the key to a successful transition.

eMazzanti leverages advanced training and close relationships with major retail technology and merchant services companies to provide your retail operation with QIR-certified EMV technologies and services and increase your technology return on investment (ROI).

Retailers have a choice in technology providers. The right retail technology partner delivers ongoing value by recommending improvements to reduce risk and keep a merchant's IT business strategy up-to-date.

[1]Kevin Woodward, (March 4, 2016). EMV Chargebacks Proving to Be a Card-Present Merchant Problem [Article]. Retrieved from http://www.digitaltransactions.net/news/story/EMV-Chargebacks-Proving-To-Be-a-Card-Present-Merchant-Problem

[2]John Stewart, (April 4, 2016). How EMV-Related Chargebacks Drove Florida Merchant Duo to Sue Networks and Issuers [Article]. Retrieved from http://t.digitaltransactions.net/news/story/How-EMV-Related-Chargebacks-Drove-Florida-Merchant-Duo-to-Sue-Networks-And-Issuers