EMV Basics & Best Practices

- Importance of EMV acceptance
- Best practices for EMV disputes
- EMV and data security

Fraud prevention takes more than new hardware – it takes knowledge and diligence.

EMV technology was designed to increase payment security and reduce fraud. It should ultimately provide a more secure payment ecosystem, but it's not foolproof. Whether you've transitioned to accepting EMV cards or not, you need to ensure you are taking preventive measures to protect your business from fraud and data breaches.

Risks of Not Enabling EMV

The potential risk to a business owner who has not transitioned to accepting EMV cards can be enormous.

Cost of a Breach

Using outdated hardware leaves you at greater risk for a breach, which costs, on average, $52,000 - $87,000 per 1,000 records. Confident you won't be breached? Don't be so sure:

- 51% of breaches in 2015 were caused by either a system glitch or human error
- 49% were caused by cyber attacks
- The percent of cyber attacks aimed at small companies has doubled since 2011

Chargeback Liability

The EMV liability shift places counterfeit and fraudulent chargeback liability on the party using the least secure technology. If you process a counterfeit or stolen card through a non-EMV enabled terminal, you are liable for that chargeback by default. These chargebacks and associated fees can add up very quickly.

Customer Frustration

As more customers get chip cards, they expect to use them as intended. By choosing not to accept EMV cards, your business runs the risk of losing customers to competitors who have made the transition to a more secure and increasingly common method of processing transactions.

Heartland

EMV Dispute Best Practices

1. Upgrade to EMV enabled equipment if possible. If your POS doesn't offer an EMV solution, you may want to invest in a stand-alone EMV enabled terminal to reduce chargeback liability exposure.

2. Train employees to spot abnormal customer behavior
   - Purchasing many large value items
   - Buying rounds of drinks or food for the restaurant
   - Opening multiple bills/tabs with different cards

3. Compare the last 4 digits on the card to the last 4 digits that printed out on the receipt. If they do not match, the sale should be voided.

4. Check the signature on the card versus the signature on the receipt. If they do not match, request proof of identification. If they still do not match, do not accept the card.

5. Review cards for legitimate features
   - Holograms of the network
   - (Visa, MasterCard, Discover, Amex)
   - Network logos
   - CVV/CVC on back or front
   - Signature line
   - Atypical size, shape, or color of card

6. Never rerun a card if it declines – for any decline reason. Always get a different form of payment.

Trust your gut, if a sale seems too good to be true or a customer's behavior is abnormal, walk away from the transaction.

EMV: Not a Magic Pill for Data Security

While EMV greatly reduces credit card fraud, it isn't enough to protect you from a data breach. Heartland Secure™ is the most secure card processing solution in the industry, backed by a comprehensive warranty. By combining EMV, end-to-end encryption and tokenization – we protect your customer's credit card data as soon as the card is used, making all card data completely useless to hackers.

- EMV chip technology authenticates that a customer's card is genuine
- Heartland's end-to-end encryption technology encrypts card data as it is entered so no one else can read it
- The encrypted data is verified by the Heartland Secure network, which replaces the data with a "token"—something of no value and unusable by outsiders
- Then the transaction is approved without ever transmitting any card data

To learn more, contact Jennifer D'Angelo:

860.659.8900 | jennifer@dangelosolutions.com | dangelosolutions.com

Heartland