Securing your Payments Processing

August 2017

October marks the two-year anniversary of the U.S. migration to EMV smart-chip enabled payment technology. Despite the fact that the migration was accompanied by a card-present fraud liability shift to the party using the least secure technology, Visa reports that only about 2 million U.S. merchants have transitioned to this new level of technology. This leaves nearly 67 percent of U.S. merchants vulnerable, as fraudsters turn their focus to non-EMV enabled businesses.

EMV, which stands for Europay, MasterCard and Visa, is the global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. EMV cards are embedded with a smart chip that creates a unique transaction code that cannot be used again, improving the payment security for consumers.

How criminals take advantage

According to the Verizon 2017 Data Breach Investigations Report, Accommodation and Food Services was "the top industry for Point of Sale intrusions." While this isn't a new problem – hotels and restaurants have been plagued by counterfeit, stolen and cloned credit card activity for years – the liability shift has further highlighted the issue.

Criminals prefer magnetic strip cards. When criminals purchase credit card numbers, the data – regardless if it is magstripe only or EMV technology – is loaded on a standard magstripe counterfeit card. If they attempt to use the counterfeit card as an EMV-enabled terminal, the terminal can detect that the card being used has EMV capabilities and the system will prompt the fraudster to "dip" the card instead of swiping. Attempts to process the transaction without "dipping" the EMV enabled card will be declined.

Some fraudsters have been scamming your businesses for years without you knowing about it because, previous to the liability shift, the issuing bank was taking the loss. All the scammer has to do now is call the credit card company after their card is swiped at an old terminal and claim the charges on their chip-enabled card weren't accurate, leaving you to empty your pockets. While the chargeback amount may not be big, it wouldn't take many of these false chargebacks to really cut into your profits. Without the ability to accept EMV transactions, business owners are seeing liability shift chargebacks for which there is no defense.

If upgrading to EMV simply isn't an option for your business, here are a few tips you can use to protect yourself from fraudsters.

- Verify that the last four digits of the card number match the last four digits on the printed receipt
- Compare the signatures on the card and receipt

- Check cards for legitimate features like holograms, logos, CVV/CID/CVV2 and AVS verification, etc.
- Never rerun a card if it declines – for any reason

Comprehensive Coverage

EMV chip technology improves security by providing card authentication. However, the most advanced credit card thieves can rewrite the magstripe, tricking even new EMV chip-reading machines to think the card is chipless when swiped. If you have purchased the EMV card-reading equipment, but are not encrypting transactions as part of your upgrade, your business may still be at risk. While EMV-enabled terminals offer increased security and reduces credit card fraud, you need to employ a comprehensive approach for the best security.

- **Tokenization** – replacing card data with a "token" protects card data while at rest in your POS system. This is particularly imperative in a hotel environment, where customer data is typically stored for days, weeks or even years. Even if your system is hacked, tokenization makes the data stored in it unusable to cybercriminals.

- **End-to-end Encryption** – this powerful technology removes card data from the merchant's network, protecting the data in transit so it cannot be intercepted or monetized.

- **Incident Management Program** – According to the Association of Certified Fraud Examiners, nearly 50 percent of small businesses fall victim to fraud as some point in their business life cycle. Every business should have a plan in place for how they will handle an incident, should one occur. Containing the breach, responding quickly and communicating appropriately is the best way to prevent reputation damage and stem losses.

Heartland Secure combines EMV, tokenization and end-to-end encryption together to give your business the most comprehensive security solution on the market. We are so confident in our ability to protect credit card data the moment it is used, we offer an unprecedented breach warranty to all merchants who are Heartland Secure and employ Heartland Secure-certified devices for as long as they are processing with Heartland, at no additional cost.

To learn how Heartland Secure could help your business protect against fraud, contact XXX.