How Merchants Can Avoid EMV Challenges

Save Time & Money by Cleaning Your Chip Card Readers

OVER THE PAST TWO DECADES, CARD FRAUD HAS HIT AN ALL-TIME HIGH WORLDWIDE – with counterfeit occurrences and card-not-present (CNP) fraud gaining or exceeding losses from traditional lost or stolen methods.

Criminals have been finding new and innovative ways to commit credit and debit card fraud since Diner's Club, Inc. introduced the concept in 1950. With well over 60 years of research and development, it should not be surprising to discover the traditional magnetic stripe system has been thoroughly outstripped.

Card Fraud in the U.S.

Fraud has migrated to less secure markets as countries have made the transition to EMV. As a result, counterfeit fraud in the United States has reached an all time high – well beyond any regularly expected year-over-year trend.

Counterfeit cards used at POS and ATMs accounted for 49 percent of all card fraud lasses worldwide in 2015, according to The Nilson Report, a leading publication covering the credit card industry. U.S. losses to counterfeiting jumped to $3.89 billion, accounting for 23.9 percent of global losses.

What is EMV Fraud Liability?

In the U.S., the EMV liability shift is not a mandate. Instead, it has been set up as a program to encourage the payments industry to invest in chip card technology. Traditionally, fraudulent transactions – no matter the source – have been the responsibility of the card issuer or the network. Now that the liability shift has taken place, any counterfeit card fraud is the responsibility of the party in the transaction chain that lacks compliance.

For POS terminals, this liability shift took place on October 1, 2015.

Research from Aite Group estimates the average loss from card skimming crime is around $50,000. POS terminals are likely to encounter rates on average of $101-$148 per counterfeit card, according to a 2013 Federal Reserve payments study.

The Mechanics of EMV Technology

The chip card technology utilized for EMV is much more complicated and takes longer than a magnetic strip transaction.

EMV relies on a tokenization process to generate a unique and encrypted authorization process. When a chip-enabled card is inserted into an EMV terminal, it makes contact with the card to power the chip and initiate a transaction. The chip card then utilizes its internal programming to package the transaction information – merchant, cost, etc. – into a one-time use encrypted code or "token" that is forwarded through the payment processing system. The token must pass through the acquirer to the network, where the information is decrypted and bank authorization is sought. Authorization or denial is then sent back down the chain.

Counterfeit cards rely on the account information pulled from merchant transaction logs, copied from the front of the card or skimmed via magnetic stripe. This information is then duplicated onto a fake version of the card for use at ATMs, POS terminals and gas pumps.

Because EMV transactions require card contact and take longer than simple swipe transactions, there is more of a chance that something can go wrong.

"The first three months of EMV in the U.S. were a learning curve for the consumer, going from mag stripe to EMV chip. Merchants who have not enabled latching on the EMV card readers should as some customers are still confused about how to use EMV and may use the new equipment incorrectly - prematurely removing their card before the chip has been fully read," said Bryant Lynch, Manager, Special Projects for Access Cash General Partnership.

When EMV Fails

Just as with magnetic stripe, EMV card readers have their failures. However, when EMV fails, retailers are capable of defaulting to magnetic stripe or manual entry. This type of transaction is referred to as "Fallback."

While not all fallback transactions will result in liability, a resulting breach can have a negative effect on brand image similar to the backlash experienced by companies such as Target, Home Depot and Neiman Marcus. The new liability rules note that if the card use to commit fraud is a PIN debit or credit card supported by MasterCard, American Express or Discover and the accepting merchant was unable to process the transaction as a chip card, the liability lies with the merchant.

Even without the threat of potential liability, most merchants have a tiered pricing model for transactions where the preferred method of payment (major credit card using EMV) results in the lowest "qualified rate" while other cards and/or types of transactions may result in less favorable "mid-qualified" or "non-qualified" rates (e.g. – "Qualified" runs at 1.5 percent, "Mid-Qualified" at 2.5 percent and "Non-Qualified" at 3.5 percent). This system creates induced penalties through higher interchange rates for every transaction processed using a fallback method.

A high level of fallback will raise red flags with the card networks. According to Visa's "Card Acceptance Guidelines for Visa Merchants." "If your key-entry or fallback rates are greater than one percent per terminal or sales associate, you should investigate the situation and try to find out why." Fallback at or above 2-2.5 percent of transaction volume will trigger a notification to the acquirer; who has 30 days to address the issue.

Payment networks are advising strong remedial action for U.S. acquirers with initial rates above a typical market migration rate of 7-20 percent. After 30 days, the network reserves the right to introduce a fine – generally in the range of $25,000 per bank identification number. Fallback rates over 50 percent have been observed regularly in the U.S. since the October 1, 2015 liability shift date.

Dealing with Device Malfunction

An EMV chip reader failure does not simply increase liability risks and raise the costs of transactions. It also incurs extra costs for evaluation and repair. Depending on the maintenance service plan, this could be the price of a technician call to the location - averaging between $100–250 per site visit.

While some service providers and manufacturers offer free replacements, merchants still face transaction loss due to a card reader being out of commission in addition to the time and effort required to submit for a replacement.

For merchants not on a free replacement plan there will be charges incurred for the repair, return or replacement of the device. In worst case scenarios, replacement systems can run anywhere from $35 for low-end or refurbished to around $1,000. However, providers are free to charge reprogramming fees or refuse to reprogram machines purchased elsewhere.

Most manufacturers and service organizations have provisions for NFFs (no fault found) and may assess additional charges, especially with repeat offenders.

While some providers and manufacturers offer free replacements, merchants still face transaction loss due to a card reader being out of commission in addition to the time and effort required to submit for a replacement.

Losing Transactions

Despite the additional costs, U.S. merchants are currently somewhat protected from more significant losses by the ability to fall back to magnetic stripe. A failed EMV transaction does not currently result in a complete transaction failure or additional laibility. However, this may not always be the case.

Visa mandated a liability shift requiring Canadian retailers to absorb fraud cost for accepting magnetic -stripe cards instead of chip and PIN after 2010. Interac set a similar mandate for 2015. After these dates, it was up to merchants to make the decision between absorbing potential liability or losing sales.

Should similar steps be taken in the United States, any fallback to magnetic stripe could leave the merchant open to additional liability.

Clean, functioning EMV chip readers are essential in order to perform business. A malfunctioning terminal could mean a significant loss in revenue – especially for smaller merchants, with only one or two card readers in-house.

Four years ago, card issuers in the U.K. determined they would no longer accept non-EMV transactions for value. Suddenly, a fallback to magnetic stripe was not an option. Clean, functioning EMV chip readers became essential in order to perform business.

The Case for Proper Cleaning

"We have found that regular cleaning of the card readers is critical to uptime," said Lynch. "Our experience has shown that the EMV chip contact degrades over time with contamination. This leads to transactions being intermittently declined by the host processor as the EMV data is incomplete."

Card readers are introduced to a large amount of oils, dirt and grime. These machines are encountering residue from consumer's cards as well as particles from the environment in which they operate. Restaurant machines are subject to additional grease, soaps and sugars. Convenience stores with gasoline operations may encounter an increase in gas or oil. Machines in food trucks, merchandise kiosks and other outdoors locales will be subject to additional dirt, dust, water and other natural elements - especially when based near roadways or other transit locations.

Cases of dirt, dust and bacteria impacting card reads are fairly significant. Terminal operators in the U.K. note levels of broken reader heads are far fewer than instances where card readers need cleaning. A 2013 study performed by NCR reported 78 percent of magnetic stripe devices sent in for card read failures were merely dirty and were returned to service after being cleaned with a cleaning card.

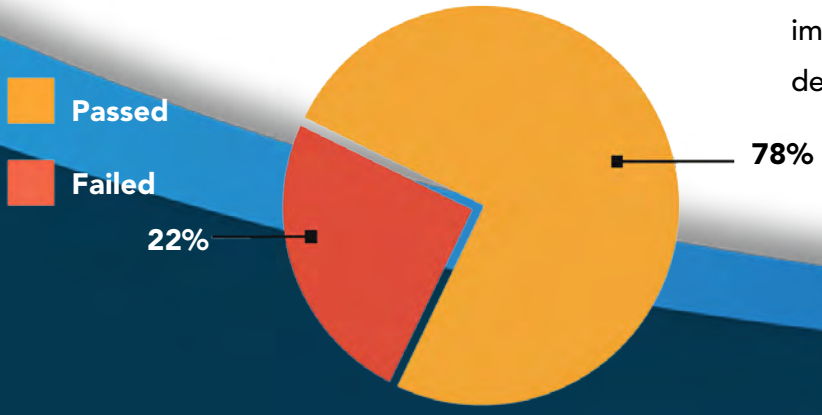
Because EMV card readers are more complex and have more moving parts, EMV readers get dirty faster and need to be cleaned more often.

"We have a cleaning arrangement as part of the preventative maintenance," said Suresh Nandihalli, COO of Euronet EFT EMEA Business. "Cleaning of the card reader…helps to reduce service calls."

Dirty card readers can lead to:

- **Increase in failed or fallback transactions**
- **Card reader errors and rejections**
- **Extended transaction times**
- **Customer frustration**
- **Poor customer experience**
- **Decreased revenues**
- **Lower shopper loyalty**

Reports from the field in Canada and Europe indicate regular cleaning of EMV card readers can impact up to 90 percent of reported fallbacks and device failures.



Industry experts agree exposure to dirt and grime, and overall usage are large factors in the break-down of card readers and recommend setting a protocols or schedules to ensure regular cleaning.

Recommended cleaning schedules by location type:

- **Indoor, Low-Use Locations**– once per week or every 1,000-2,000 transactions
- **Indoor, Low-Use Locations Where Food is Served** – twice per week or every 500-1,500 transactions
- **Indoor, High-Use Locations** – twice per week or every 500-1500 transactions
- **Outdoor, Low-Use Locations** – twice per week
- **Outdoor, High-Use Location** – once per day

[Outdoor Locations include fairs and festivals, food trucks, gas pumps and other outdoor merchants]

Avoid EMV Pitfalls

Malfunctioning EMV card readers are costly – leading to increased transaction charges and additional service and repair fees. However, the majority of faulty card readers do not truly need repair, they merely need to be properly cleaned. Implementing appropriate protocols or scheduling for regular card reader cleaning, utilizing low-cost cleaning cards, can significantly improve reader performance – resulting in fewer failed or fallback transactions, a decrease in errors, faster transaction times and greater customer satisfaction.