Currently, EMV chips are globally adopted as a standard for authenticating debit and credit cards. EMV stands for Europay, Mastercard, and Visa. EMV technology is now widely adopted and relatively common all over the world. Many cards still use the previous technology, with a magnetic strip on the side – but most of them now also include rectangular chip, called the EMV chip.

The technology was widely adopted particularly because of two reasons, i.e., it is more secure and also major credit card companies shifted fraud liability from themselves to business owners without EMV.

**How Magnetic Stripe Cards Were Replaced with EMV Cards**

Magnetic stripe cards store digital data for making payments. This method was inexpensive and secure, with fast checkout. The technology works on ‘security through obscurity’, which means that your payments are kept safe by keeping confidential the internal design architecture. However, over the time, the equipment used for reading and writing these strips became easily accessible. The internal design architecture could be easily accessed and replicated, which removed the ‘security through obscurity’ protection. Counterfeit cards were made by easily reading and reproducing magnetic stripe cards, which greatly reduced the once prominent security feature of these cards.

During this time, Europe quickly adopted [EMV chip](http://www.cardzgroup.com/ContactSmartCard.html) technology, as it provided next-level security to card transactions, thus solving all security issues faced by magnetic stripe cards. The US was slow in adopting the technology, since not only was it expensive but also took time by customers to be accepted. However, with time the security benefits outweighed all these concerns and EMV became a widely-adopted technology.

**How EMV Chip Payments Works**

Just like magnetic stripes, EMV chips have information that is needed for processing payments. But the microchip has more information that is also kept encrypted. Due to the encryption, criminals cannot use data reading technology and devices for stealing cardholder data. However, for this to work, the Point of Sale (PoS) device accepting the card should have the ability to read and process the data on the microchip.

The encryption works by the card producing a unique token or code for each transaction. Instead of the cardholder’s real information, the token is transmitted during the payment process. In 2019, Visa reported that there was a decline of [87 percent in counterfeit cards fraud due to EMV technology](https://www.pymnts.com/visa/2019/visa-chip-cards-reduced-counterfeit-fraud-by-87-pct/).

Traditional credit and debit cards can be read easily through skimming techniques, whereas a PIN and chip provides stronger authentication. EMV card payments need one Triple-DES unique key along with one of the secure data encryption and card authentication mechanisms, i.e., dynamic data authentication, static data authentication, and combined data authentication – along with a compatible Point of Sale terminal.

Let’s have a look at seven ways EMV chips payments improve security.

## Fraud Prevention

EMV chips are designed particularly for preventing fraud. Magnetic strips were designed for making transactions easier for customers, whereas EMV chips took this technology a step further and added an extra factor of fraud prevention to card payments. Statistics also show that in-person credit card fraud cases declined after the introduction of EMV chips.

## Encryption

## When using magnetic stripe cards, payment information is broadcasted directly to the bank. However, when using EMV chip card, the information is encrypted by scrambling and sent to the bank in a language that can only be deciphered by the bank’s software. This process cuts down significantly on fraud, as it makes it nearly impossible for cyber criminals to intercept exchange of information between the bank and the card.

## Unique Transaction Codes

## Each transaction that takes place generates a unique code that cannot be reused. In contrast to this, information on magnetic strips can be cloned by a scammer and used repeatedly. In case of EMV cards, even if hackers get the code information, they cannot use it, since the code is different every time.

## Almost Tamper Proof

## Tampering with chip cards is very difficult. With magnetic strips, it costs very little to make skimmers and install them on ATM devices to capture all credit card details of users. However, EMV chip cards use small computer chips that are not easy to counterfeit. To copy such information from these cards, hackers need equipment that costs almost a million dollars, which is something most scammers are unable to afford.

## Conclusion

## On a final note, when running a financial institution, it’s important to know that there is no technology that guarantees hundred percent security. Although EMV chip cards are more secure as compared to magnetic stripe cards, it can still not protect customers from all kinds of data breaches, such as card-not-present fraud (when purchases are made by phone, online, or through mail order). We still need to take necessary precautions to keep the customer’s banking and credit card information safe.