How credit cards with EMV (chip) work

POSTED BY: BRENDAN BYRNE  1 DAY AGO

The credit card has fast evolved over the years to replace the traditional mode of payment. With its increased acceptability and the convenience it offers, it is not surprising that nowadays a preponderant number of people use a credit card of different types and functions. Sometimes users are attracted to the travel rewards credit card that offers its users redeemable points, miles that can be used to reduce the cost of an airfare payment, or even the option to drive down debt with credit cards specifically for balance transfer.
Irrespective of what kind user you are, whether you are a lackadaisical user who only remembers that he has a credit card when he stumbles on it or the kind of user with more credit cards than you can count, your issuer has definitely made sure that by now all your valid credit cards have the EMV (chip) technology. Just like the old ones they replaced, this new one still has the Magstrips ensuring that they are compatible with older card readers. **Card issuers and Tech enthusiasts** believe that chip cards payment **technology** have come to stay.
Q2 hedge fund letters, conference, scoops etc

One of the reasons why the issuers switched from the old, magstripe only credit cards was because the issuers were constantly outmatched by cybercriminals. In 2013, hackers stole 45 million dollars, due to breaches with bankcards. Hackers seemed more sophisticated and equipped than the card issuers. This led to a series of brazen hacking attacks resulting in untold mental pain for the regular Joes and Janes caught up in the turmoil. Card issuers have to constantly work to eliminate data breaches as incentives to steal financial information are powerful.

Due to the economic strength of the United States, the country has become a preferred target for hackers seeking to get some financial benefit or make a statement for their cause. According to the Nilson Report credit card fraud reached $16.31 billion in 2014, and the U.S. accounted for 48.2% or $7.86 billion of gross card fraud worldwide. The lack of EMV-compliant infrastructure was blamed for this staggering figure.

The EMV is an abbreviation for “Europay, MasterCard, and Visa”. The named was culled out of the credit card networks that spearheaded the development of this protocol. An impartial consortium was formed; the members consisted of those three that developed the protocol, joined by China UnionPay and JCB. The name of the consortium is EMVco, they facilitate a worldwide acceptance of secure payment transactions and interoperability of secure payment transaction worldwide. The consortium also evolves the EMV chip specifications and related testing processes, but does not in any way enforce EMV compliance within a
marketplace which is the responsibility of the marketplace regulatory body. The EMV card is now a widely accepted technology for securing payment cards.

**How EMV card technology works**

The difference in the EMV chip transaction and magnetic stripe is basically in how it functions. The traditional magnetic stripe is a data store which contains information that can be used just once when it is read by the terminal, it becomes just an ordinary plastic and should be discarded while the EMV chip is more of an intelligent chip. The EMV chip processes information and can determine the outcome of transactions based on pre-determined rules by the card issuer. The EMV chip enforces rules like offline data authentication, online authorization, verifying the identity of the cardholder by pin and any other verification that the issuer deems necessary. The information in the EMV chips are dynamic and can change with every transaction, those with magnetic stripe cards don’t have that luxury as the information on the magnetic stripe were static, once in it, it can’t be changed. The interaction between the chip and the terminal seem short but many processes occur within that short time. Every new transaction you initiate produce a unique code (usually called token) with a principle called cryptography, this principle is very similar to the complex mathematical design used for cryptocurrency, the introduction of cryptography to financial technology brought a great deal of safety to finance, to learn more about cryptography, click [here](#). The token code generated is unique to that transaction and it is ensured that no two transaction codes are ever the same, past, present or future.

For every transaction initiated by EMV, a two-key triple DES cryptography will generate an application cryptogram. The cryptogram generated for online
authorization request in called Authorisation Request Cryptogram (ARQC), when the transaction is declined, the cryptogram generated is known as Application Authentication Cryptogram (AAC). The cryptogram generated by signing data elements when the payment is approved for clearing and settlement is called a Transaction Certificate (TC).

Authorization controls and risk management

The EMV chips are designed by card issuers to give some degree of controls to the issuing bank. The chip transaction gives banks point of sales controls, so as to reduce the level of exposure to fraud for the cardholder. Banks can set limits that cap the number of consecutive offline transactions that may be processed. In some countries, banks limit the volume of transaction that can be done in a 24 hour period, any transaction you wish to process that is above that cap will require you to contact your financial institution. Depending on the preserved risk of exposure, the financial institution can issue a script commands that limits the amount of money that be withdrawn to zero. They can also issue scripts to block or disable a card based on terms and agreement.

This measure helps to reduce the loss of funds in the event of a stolen or lost card.

Cardholder Verification

The EMV chip built on the successes of the magnetic stripe only card verification system, its failures were studied and modified, new features were also added. The two new features that were introduced gave issuers the responsibility and flexibility in determining and enforcing methods for verifying cardholders.
The two features are

- Cardholder verification method (CVM) List
- Offline Pin

**CVM List:** The CVM list allows issuers to determine the cardholder verification methods and the order of priority to be used for specific acceptance conditions, thus allowing the terminal to carry out cardholder verification if it supports the feature. And if it doesn’t, it provides an alternative.

**CVM offline PIN:** A cardholder can verify a pin entered into the terminal PIN pad offline, this method dual-pin verification is quite new as it was launched with the EMV chip. The use of Offline pin is entirely optional to the issuer.

Without any doubt, card issuers migrating to EMV Strips is a smart move, as EMV has significantly reduced card-present fraud in the world, little wonder the gradual acceptance of this technology, based on EMVco Report for Q4 of 2018, 73.6% of the world transaction are via EMV.
Markets are volatile. Rates are uncertain. This is the time for innovative income-generating investments.
Brendan Byrne

While studying economics, Brendan found himself comfortably falling down the rabbit hole of restaurant work, ultimately opening a consulting business and working as a private wine buyer. On a whim, he moved to China, and in his first week following a triumphant pub quiz victory, he found himself bleeding on the floor based on his arrogance. The same man who put him there offered him a job lecturing for the University of Wales in various sister universities throughout the Middle Kingdom. While primarily lecturing in descriptive and comparative statistics, Brendan simultaneously earned an Msc in Banking and International Finance from the University of Wales-Bangor. He's presently doing something he hates, respecting French people. Well, two, his wife and her mother in the lovely town of Antigua, Guatemala. To contact Brendan or give him an exclusive, please contact him at theflask@gmail.com
ValueWalk Comment Policy
No spam, scams, illegal activity, profanity, personal info etc.
Please read our Comment Policy before commenting.