ATM CVV1 + Service Code, POS Security Flaw?

Asked 4 years, 6 months ago Modified 4 years, 6 months ago

Viewed 1k times

-1

I'm new to this topic and I found it very interesting how all the payment system is currently working. To be honest it look like they are not doing enough to stop fraudulent activity with Credit Cards.

From my understanding, each card has an smart chip that use encrypted data, this to overcome the Magstrip plaintext.

The problem that each card STILL has a Magstrip in case EMV is not working(Merchant don't wanna lose customers).

When the POS cant read the Chip, it will fallback to the Magstripe. What criminals are doing is cloning track 1//2 on Mag cards with blank/unreadable Chip, this will cause the POS to fallback to Magstripe transaction... and the whole EMV is irrelevant in this case.

I thought this is extremely dangerous and went to the wild to check it on my own card(201 / Chip and Pin) and here is the outcome:

I cloned my own CC (201 / chip) on blank Magstripe card and went to the ATM.. after typing the PIN i got the withdrawal screen, pressed on the lowest amount then the ATM said "Service is Unavailable for this card".

Then I did some research and found this : https://github.com/samyk/magspoof/pull/3

I know that when changing the service code, the CVV1 is also changed (DES encryption of PAN, Exp Date and Service code = CVV1). But I changed it to see what will happen.

Its so weird, The cloned card of my own CC worked just on 1 model of ATM. I even tried to change the CVV1 to random number and its still working on that specific ATM(My bank is not even checking CVV1 ????)

Does anyone know whats going on? Why when changing the Service Code its working on 1 Model of ATMS? Why my bank is not verifying the CVV1 value?

Can someone please explain why my own cloned card is not working when using 201 as service code? The POS should do fallback transaction as he cant read the Chip.

Its really confusing and scary at the same time, how this simple trick (Changing 201 to 101), made the POS to continue the transaction, and then the bank didnt even verify the CVV1(I even typed 000 then random number and still it works).

Should I report this to my bank/POS company?

security credit-card emv credit-card-track-data

Share

Improve this question

Follow

asked Jun 8, 2020 at 20:21

Moudilan999

1 • 2

1 Answer

Sorted by: Highest score (default)

0

The magnetic stripe is still placed on the card since EMV migration is not 100%, and is expected to go away. However, there is a concept of the liability shift - the end which uses lowest technology has to take the hit in case of fraud. If the issuer is a fully EMV compliant and if the acquirer is not, then in case of a chargeback acquirer loses, same the other way.

But the case of CVV not verified looks a bit strange since every bank will do CVV validation.POS company can't do anything here since they have no way of saying the CVV is correct or no without CVK, which is only with the issuer. You can certainly report this to the bank.

But make sure you do these simulations in live systems with caution as you can get considered a fraudster for skimming the card, even if it is your card.

Share Improve this answer

Follow

answered Jun 20, 2020 at 19:44

Adarsh Nanu

2,211 ● 1 ● 14 ● 20