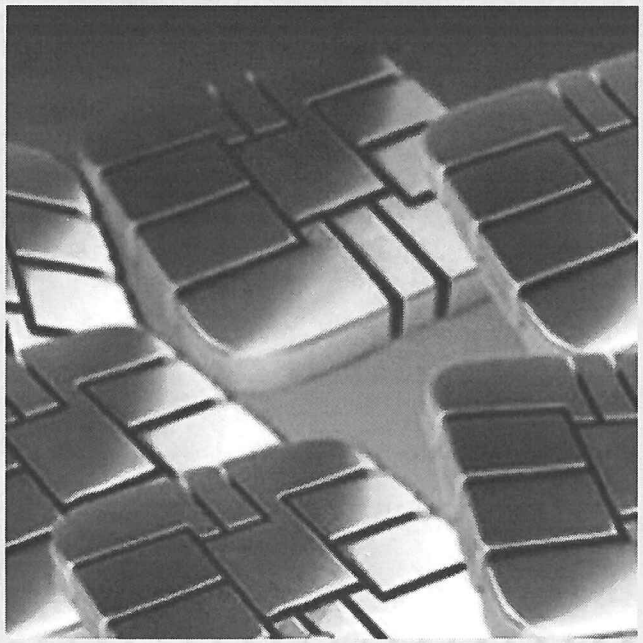


January 20, 2016
House Committee on Financial Services
David Q. Worthams, Policy Director

EMV (AKA CHIP AND PIN) CARDS AREN'T THEY THE BEST! (OR ARE THEY?)

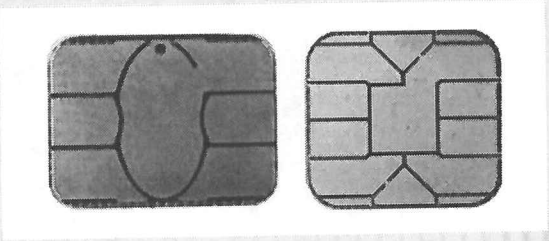
mba
Michigan Bankers Association

A QUICK HISTORY OF CREDIT CARDS

- 1951 – Franklin National Bank (in New York) introduces bank credit card
- 1958 – Bank of American begins *BankAmericard*
  - Establishes fees to pay for the service
    - Annual Fee – paid by card users
    - Interest Rates – paid by card users
    - Per Transaction Fees – paid by merchants
- 1966 – BankAmericard & the InterBank Card Association (which will eventually become Mastercard) allow other banks to use cards as *franchisees.*
- 1970 - BankAmericard becomes a multiparty corporation that eventually becomes VISA
  - Sets first interchange fee at 1.95% per transaction
  - Fee eventually set at $.42 per transaction
- 1988 – The first nationwide PIN-debit provider is launched
- 2015 – Financial Institutions are required to offer cards equipped with chip-based technology.

mba

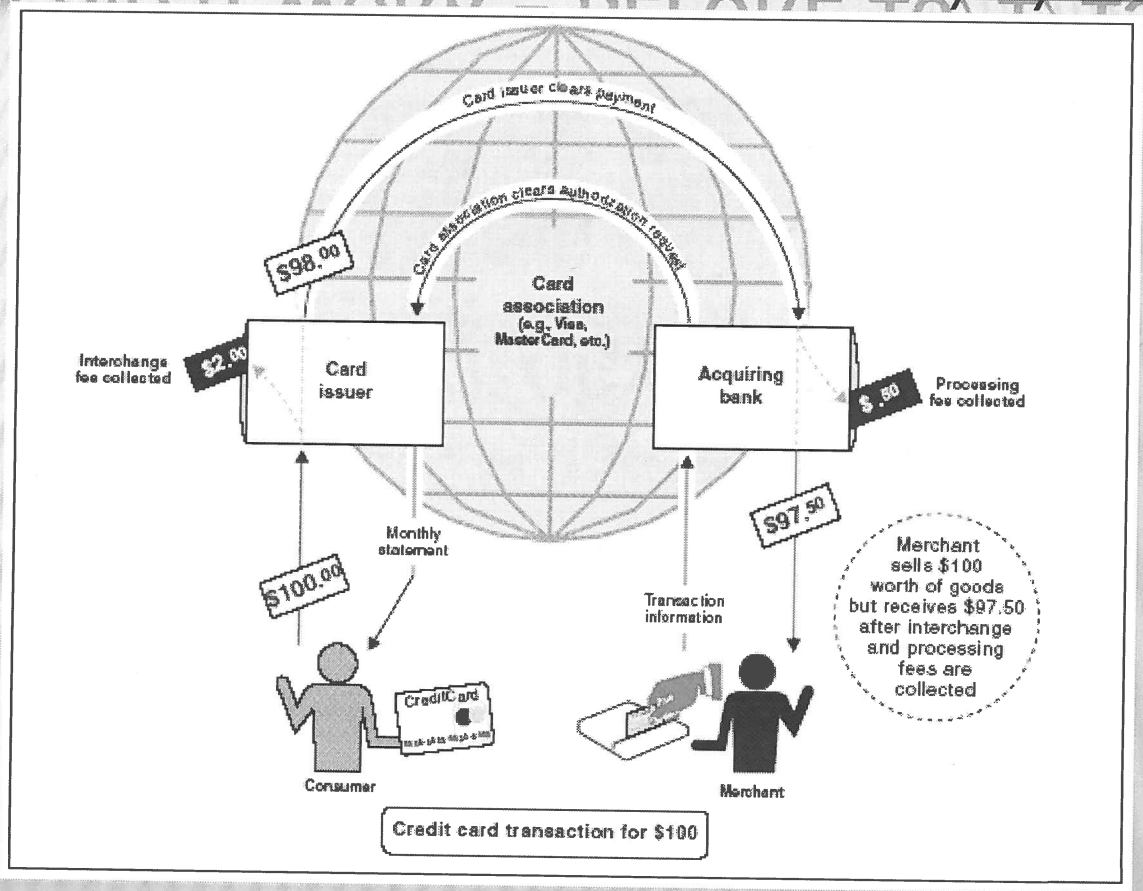
EMV CHIP TECHNOLOGY – WHAT IS IT?



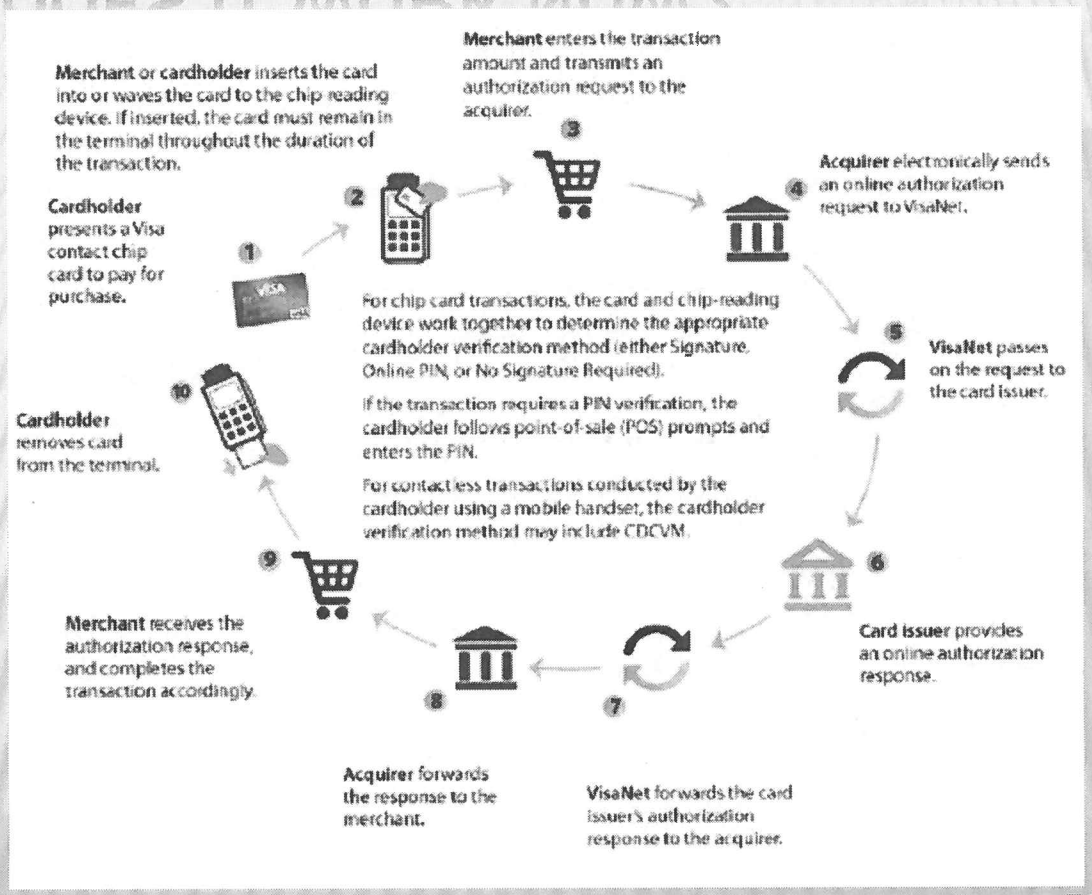
- Debit/Credit cards with EMV (Europay, MasterCard,Visa) include a microprocessor "chip" that protects personal information
  - Generates a unique, random set of numbers to complete each transactions
  - These cards are more secure than magnetic stripe cards.
  - Consumers continue to have zero liability for fraudulent transactions

mba

HOW DID IT WORK – BEFORE 10/1/15



HOW DOES IT WORK NOW?



THE U.S. ROLLOUT OF EMV

- 2012
  - Visa, MasterCard, American Express, Discover all announce EMV migration plans
- 2013
  - Processors required to be ready for and provide support to merchant use of EMV Chip transactions.
  - MasterCard also requires EMV compliance at all U.S. ATM's.
- 2015
  - On October 1st - Liability shifts to the party that is the cause of an EMV chip transaction not occurring. Does not include automated fuel dispensers (i.e. gas pumps)
  - Visa also requires ATM's to support EMV Chip transaction data
- 2016
  - MasterCard shifts liability for all U.S. ATM's
- 2017
  - Automated fuel dispensers must comply with EMV requirements
  - Visa shifts liability for all U.S. ATM's

mba

BANKS ARE READY FOR EMV

- 575 Million chip cards were in use in the U.S. by the end of 2015
  - This is the most of any other country in the world
- 3 out of every 5 people have EMV in their wallet
- 80% of shoppers believe that retailers should be held to the same security standards as banks.
  - Moving to EMV helps market move in that direction.

mba

LIABILITY SHIFTS – IN GENERAL

Card Type	Point of Sale (POS) Capability	Who's Liable
Magnetic stripe only	Terminal not enable for contact	Card issuer (i.e. financial institution)
Magnetic stripe only	Chip reader ready & enabled	Card issuer
Chip	Chip reader ready & enabled	Card issuer
Counterfeit magnetic strip with track data copied from a chip card	No chip reader (or chip reader not enabled)	Merchant
Counterfeit magnetic strip with track data copied from a chip card	Chip reader ready & enabled	Card issuer

IN SHORT – WHICHEVER PARTY HAS THE LESSER TECHNOLOGY WILL BEAR THE LIABILITY

mba

WHY THE MOVE TO EMV

- 25% of the world's payment card transactions are generated in the U.S.
  - More than 50% of card fraud in the world occurs here too
- $10 billion in card fraud losses in 2015
  - The rate has doubled in recent years
- Europe experience a 27% decrease in card fraud since EMV rolled out in 2007

mba

SO CHIP AND PIN MAKES EVERYTHING ALL RIGHT, UPTIGHT AND OUT OF SIGHT?

WE'RE NOT THERE YET

- EMV is more secure
  - Additional layer of security
  - Virtually impossible to duplicate a card with a chip
  - Increased encryption is effective in combating credit card fraud
  - Should prevent personal data from being stolen

- BUT
  - Chip only works at a business that has a chip-enabled terminal
  - No single technology will prevent fraud
  - EMV is just a part of the greater effort being made by banks and credit networks to combat thieves and hackers
  - Hackers have already discovered ways to break EMV's algorithms
  - EMV chip and pin cards do nothing to prevent Target and Home Depot type of breaches

mba

THE PRE PLAY ATTACK

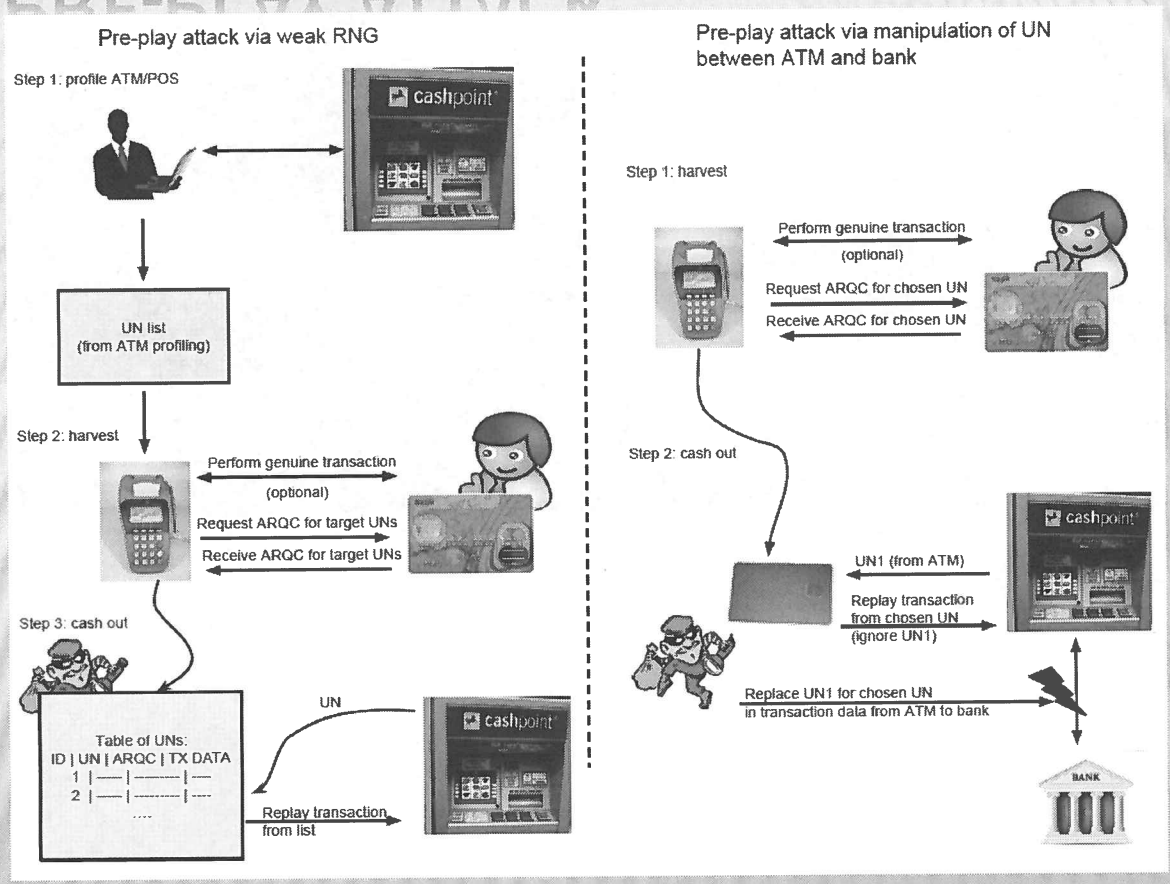
- Researchers at Cambridge have discovered that the code for each transaction is not truly unique.
  - *"Some EMV implementers have merely used counters, timestamps, or home-grown algorithms. This exposes them to a 'pre-pay' attack which is indistinguishable from card cloning from the standpoint of the logs available to the card-issuing bank, and can be carried out even if it is impossible to clone a card physically"*

  Mike Bond "Chip and Skim: Cloning EMV cards with the pre-play attack", Sep. 12, 2012

- An EMV based on a weak random number generator (RNG) can lead to similar fraud seen in the Target/Home Depot data breaches.

mba

THE PRE-PLAY ATTACK



IS A PIN MANDATE THE SOLUTION?

NO, IT ISN'T

- Consumer protection will not increase with PIN mandates
  - Static PINs are incapable of thwarting sophisticated hackers
  - PINs do not encrypt any data
  - There continues to be "zero liability" in the card issuers contracts.
  - Banks and Credit union are covering the cost of making consumers whole when impacted by a data breach
  - Even the Consumers Financial Protections Bureau (CFPB) opposes a PIN mandate
  - 50% of U.S. transactions are "no verification needed" transactions because the cost of the sale is too low to require PIN or signature.
- Most frauds/data breaches come at the retailer level.
  - PINs have been stolen and used to clean out accounts before a breach is even discovered by a retailer.

mba

TOKENIZATION – THE NEXT STEP

- An important feature that mobile wallets use
  - Apple Pay
  - Google Wallet
- Works by replacing sensitive consumer account information (both at cash register and online) with a random string of letters, characters, and numbers.
- Only used for one transaction and then is rendered useless

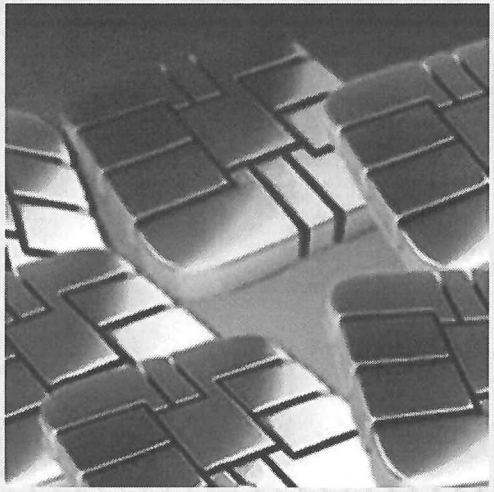
SMART SECURITY IN AN EVER CHANGING WORLD

POLICY OPTIONS

- Protect The Entire Payment system
  - With non-banking institutions offering ways to pay, it is imperative that they are subjected to the same requirements as banks.
  - Thieves move to the most vulnerable spot in the payment system
- Support Collaborative Efforts to Stop Cyber Crimes
  - **Michigan State Police Michigan Cyber Crime Division**
- Create Environment for Advances in Cyber Security

mba

INNOVATE DON'T MANDATE



January 20, 2016
House Committee on Financial Services
David Q. Worthams, Policy Director

EMV (AKA CHIP AND PIN) CARDS AREN'T THEY THE BEST! (OR ARE THEY?)

mba