



Card Payment Systems

The Fiserv logo, consisting of the word "fiserv." in a large, orange, sans-serif font, with a white swoosh graphic underneath.

MVL Consulting Private Limited
www.mvlco.com

Program process

- Inter-active sessions
- Post program support
- Reviews/questions during the sessions
- If you do not understand, ask immediately
- Speed of delivery
- Mobile phones
- Session breaks



Card Payment Systems

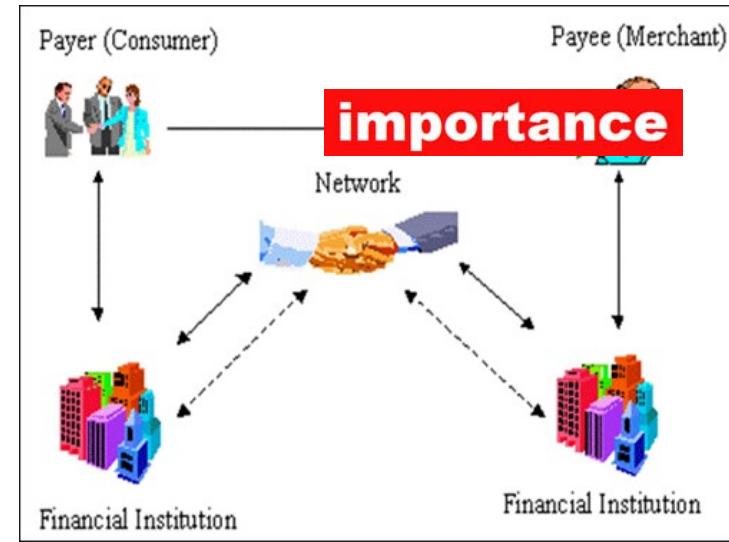
Module 1
Basics of Card Payment Systems

MVL Consulting Private Limited
www.mvlco.com

Key elements of payment

- **Message**
 - instructions or request to pay
- **Clearing**
 - message processing, may involve netting
- **Settlement**
 - exchange of value between parties

- **A card payment transaction has all three elements**
 - (1) Message (2) Clearing/Netting (3) Settlement
- **Payment system classification**
 - Whole sale and retail payment system
 - Real-time and batch payment system



Brief history

- **1887** : The concept of using a card for purchases was described



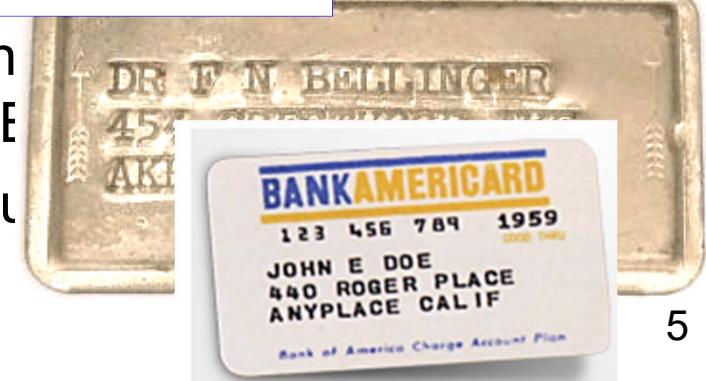
founders of Diners Club

- **1951** : The Franks brothers founded Diners Club and introduced charge cards.
- **1958** : Bank of America

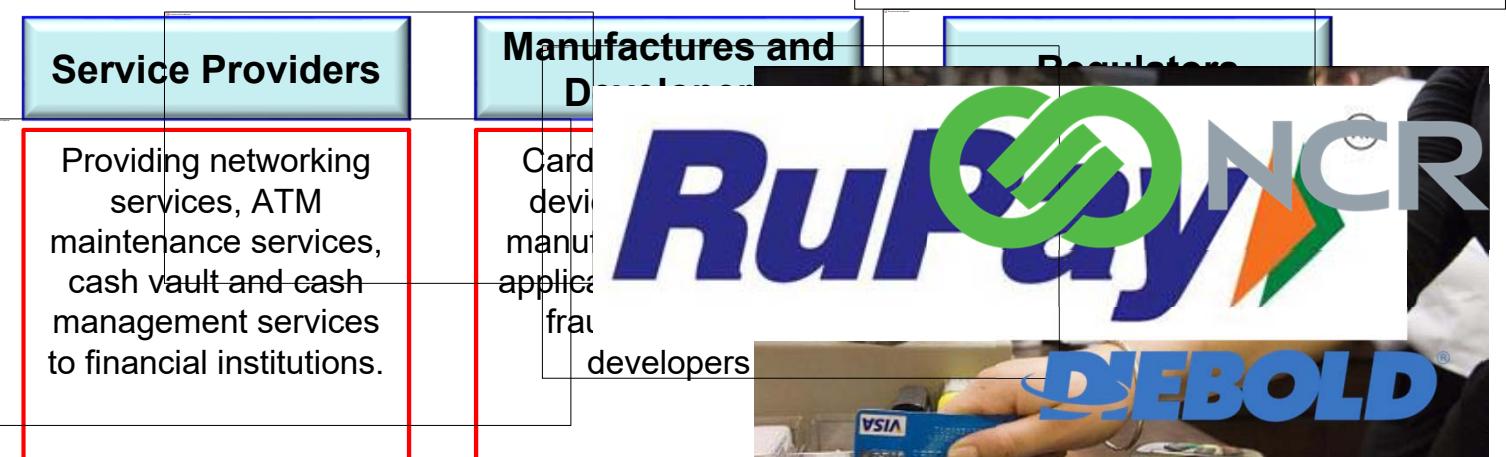
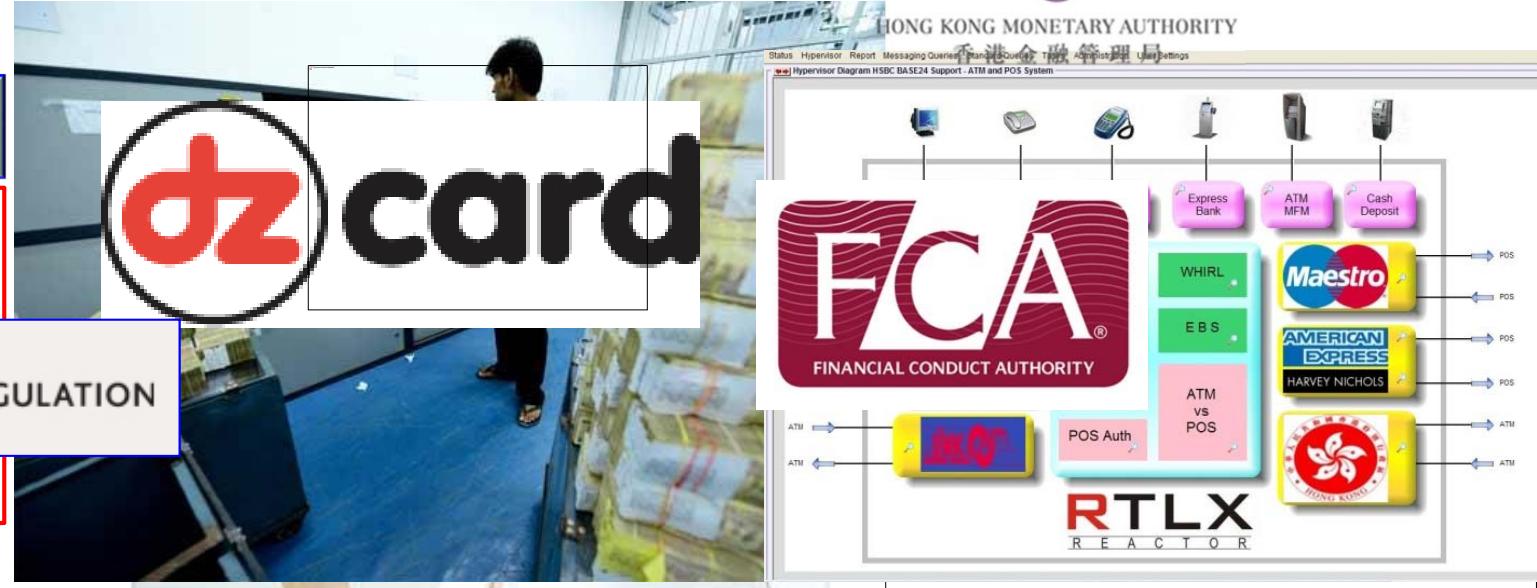
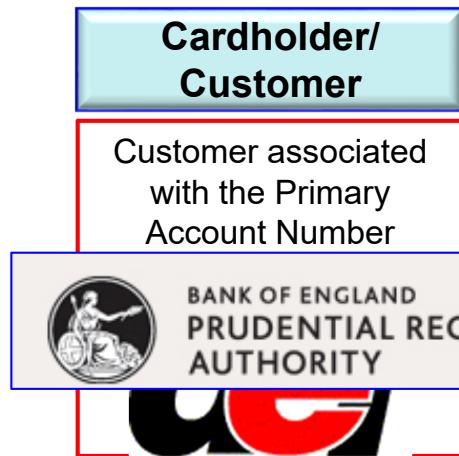


MasterCard was born in 1966 to compete with BankAmericard. The United Kingdom launched its own card in 1968.

www.mvlco.com



Players in Payment Card Industry (PCI)





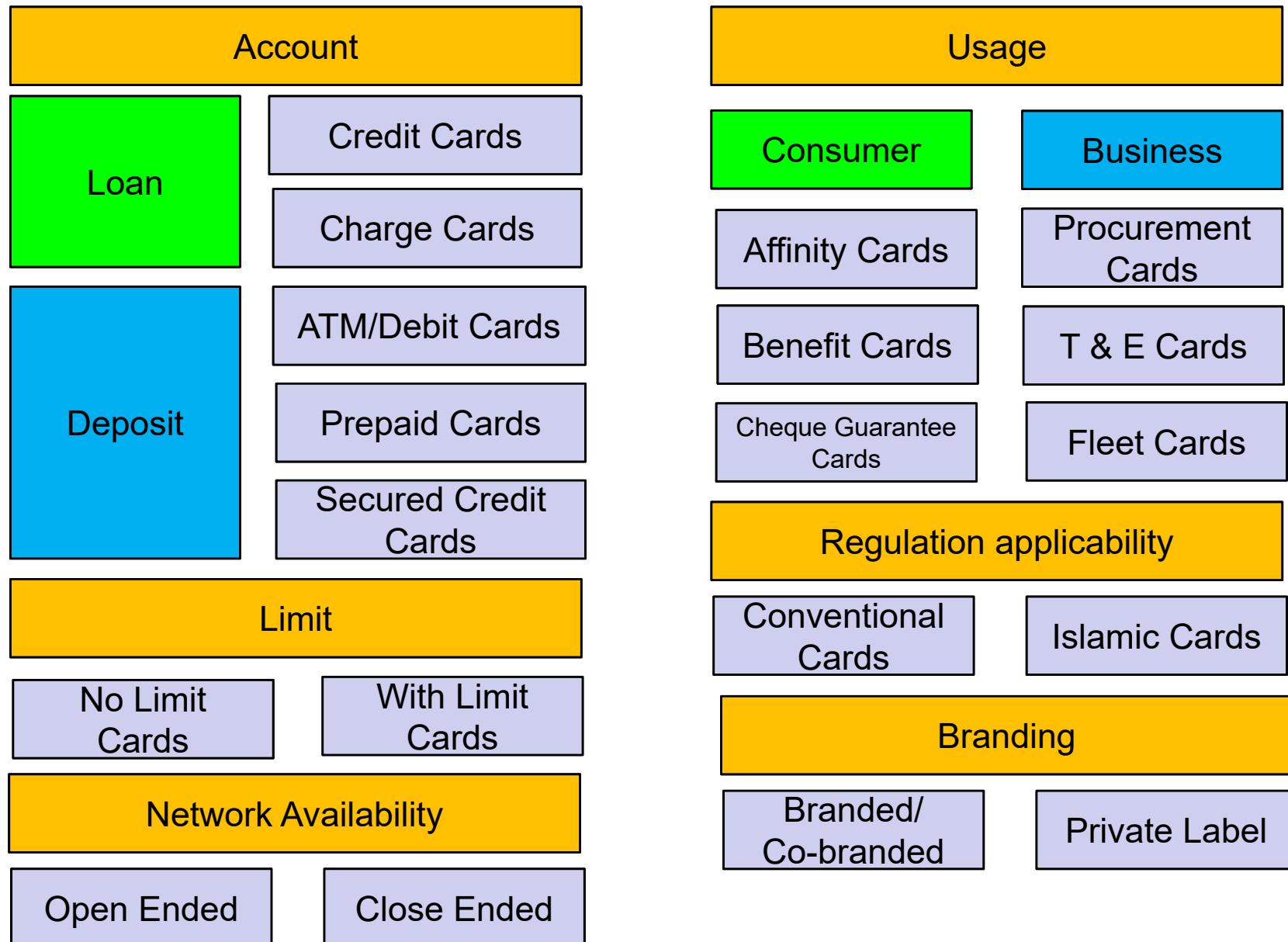
SCHEMES AND TYPES OF CARDS - PRODUCTS

Card schemes

- **Three party scheme**
 - There is only one player dealing with the customer and the merchant
 - Example : American Express, Diners Club, Discover
- **Four party scheme**
 - Customer
 - Issuer
 - Acquirer
 - Merchant

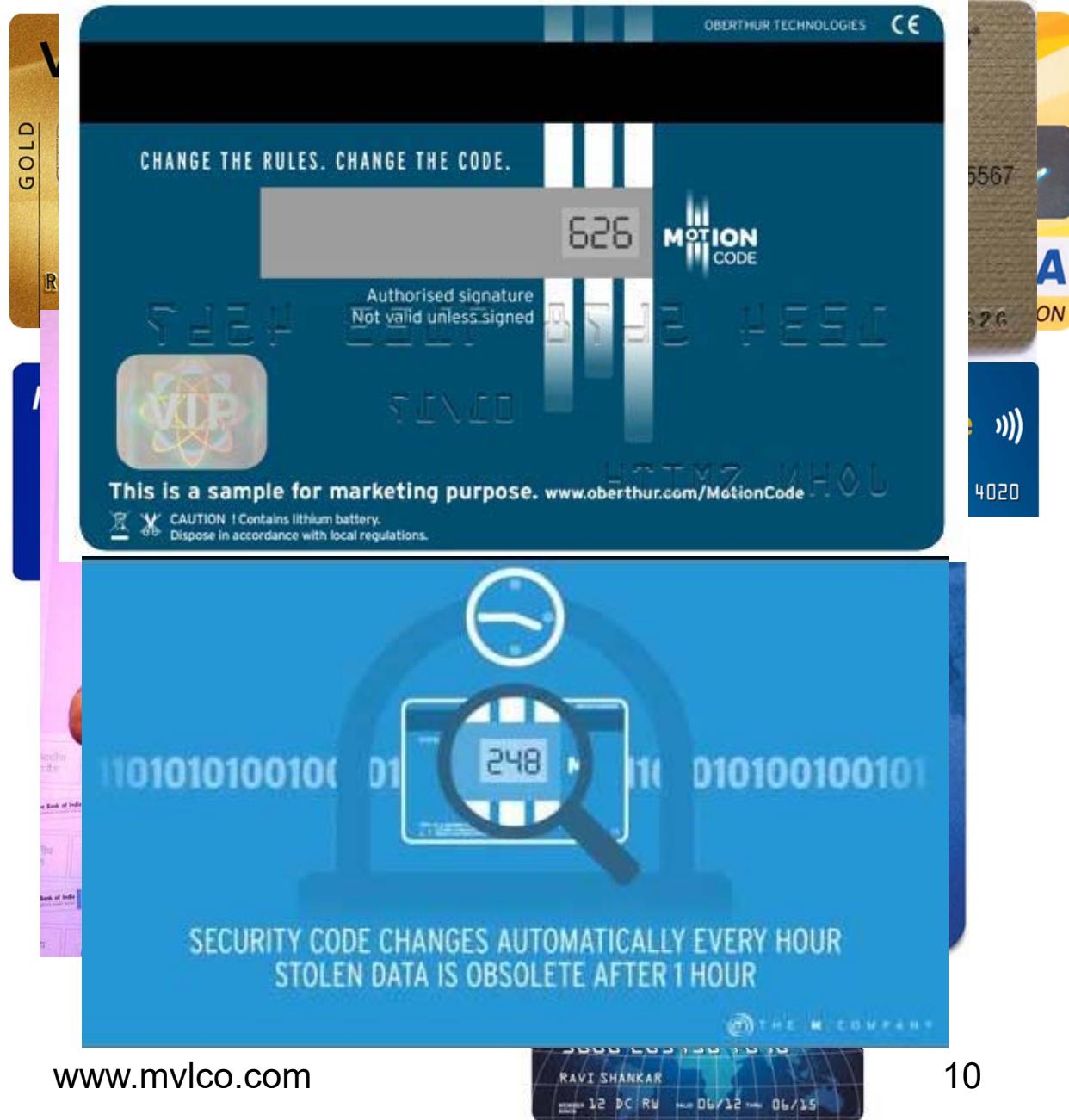


Card classification



Various card brands

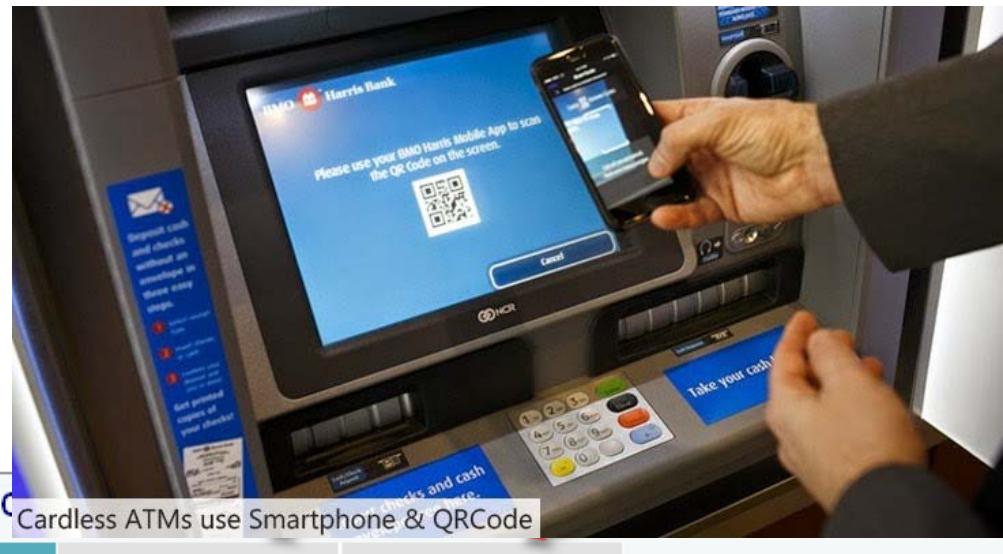
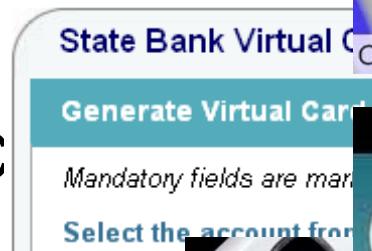
- Visa
- Visa Electron
- Visa Paywave
- MasterCard
- MasterCard Electronic
- MasterCard Maestro
- American Express
- Diners Club
- JCB
- Discover
- Rupay
- Many more....



Card classification

ISO 7810/ISO 7816

- Magstripe Cards
- Smart Cards – Chip or ICC
- Contactless Cards
- NFC Cards
- Virtual Cards
- Quick Response C



Micro module metallic chip design



- VCC: power supply
- RST: reset signal, used to reset the card's communications
- CLK: provides the card with a clock signal
- GND: ground (reference voltage)
- VPP: designated this as a programming voltage
- I/O: serial input and output (half-duplex).
- C4, c8: the two remaining contacts are used for usb interfaces and other uses

C1	Supply voltage (VCC)	C5	Ground (GND)
C2	Reset (RST)	C6	RFU ²
C3	Clock (CLK)	C7	Input/output (I/O)
C4	Not used; need not be physically present	C8	Not used; need not be physically present

Micro module metallic chip design



- VCC: power supply
- RST: reset signal, used to reset the card's communications
- CLK: provides the card with a clock signal
- GND: ground (reference voltage)
- VPP: designated this as a programming voltage
- I/O: serial input and output (half-duplex).
- C4, c8: the two remaining contacts are used for usb interfaces and other uses

C1	Supply voltage (VCC)	C5	Ground (GND)
C2	Reset (RST)	C6	RFU ²
C3	Clock (CLK)	C7	Input/output (I/O)
C4	Not used; need not be physically present	C8	Not used; need not be physically present

Card Payment Systems

Module 2
Understanding Card and PIN

MVL Consulting Private Limited
www.mvlco.com

INTERNATIONAL STANDARD

ISO/IEC 7812-1



Hans Peter Luhn

Hans Peter Luhn was a researcher in the field of computer science for IBM, and creator of the Luhn algorithm, KWIC indexing, and Selective dissemination of information. [Wikipedia](#)



Born: July 1, 1896, Barmeren

Died: August 19, 1964, Armonk, North Castle, New York, United States

Fields: Computer Science

Institution: IBM

- Luhn Algorithm (mod 10) can be used for number validation.

Card backside

CVV2/CVC

Ch
W
is
mu
45
act
pa

Sig
dra
sig
pa



CVV2



CVC2



CID



CID



CID



Data Element	Track 1	Track 2
Start sentinel	X	X
Format code="B"	X	X
Primary account number	X	X
Field Separator	X	X
Name	X	
Field Separator	X	X
Expiration date	X	X
Service code	X	X
Discretionary data	X	X
End sentinel	X	X
Longitudinal redundancy check	X	X

CARD TRACKS DATA

Figure A-1: Track 1 Record Format

Field Number	Length	Field Name
1	1	Start Sentinel
2	1	Format Code
3	13 or 16	Primary Account Number (PAN)
4	1	Separator
5	2 to 26	Cardholder Name
6	1	Separator
7	4	Card Expiration Date
8	3	Service Code
9	0 or 5	PIN Verification
		Position Length Content
		1 1 PIN Verification Key Index PVKI
		2 to 5 4 PIN Verification Value (PVV)
10	Varies ¹	Discretionary Data
11	11 ²	Visa Reserved
		Position Length Content
		1 to 2 2 Zero fill
		3 to 5 3 Card Verification Value (CVV)
		6 to 7 2 Zero fill
		8 1 Authorization Control Indicator (ACI)
		9 to 11 3 Zero fill
		All 11 positions are required
12	1	End Sentinel
13	1	Longitudinal Redundancy Check (LRC)

SAMPLE

Table B-1: Track 2 Record Format

Field Number	Length	Field Name
1 ¹	1	Start Sentinel
2	12–19	Primary Account Number (PAN)
3	1	Separator
4	4	Card Expiration Date
5	3	Service Code
6	0 or 5	PIN Verification Data
7	varies ²	Discretionary Data ³
8 ¹		End Sentinel
9 ¹	1	Longitudinal Redundancy Check (LRC)

¹ Fields 1, 8 and 9 are not sent in online messages but are necessary for magnetic stripe-reading devices.

² The length depends on the lengths of fields 2 and 6. Refer to the Data Element Descriptions later in this appendix.

³ Contains the 3-digit Card Verification Value (CVV) or optional iCVV on a chip.

PIN

- The minimum PIN length is 4 digits. For verification in interchange transactions, the maximum PIN length is 6 digits. An issuer can elect to support longer PINs upto a maximum of 12 digits as specified in ISO 9564.
- PIN types
 - Assigned derived PIN
 - Assigned random PIN
 - Customer selected PIN
- Implicit PIN activation/Explicit PIN activation
- PIN block formats



Card Payment Systems

Module 3 Before Starting Card Operations

MVL Consulting Private Limited
www.mvlco.com

Before starting card operations

- Switch
- Host – Core Banking Solution/Credit Card Server
- Host Security Module (HSM)/Software Security Module (SSM)
- Network
- Devices
 - ATM
 - POS
 - Websites
 - MOTO
- Card production and management system
- Authorisation management system
- Fraud management system
- FX rate feed system
- Billing system
- Call management system
- Cash management and forecasting software
- Backup system

Card Payment Systems

Module 4 Transaction Processing

MVL Consulting Private Limited
www.mvlco.com

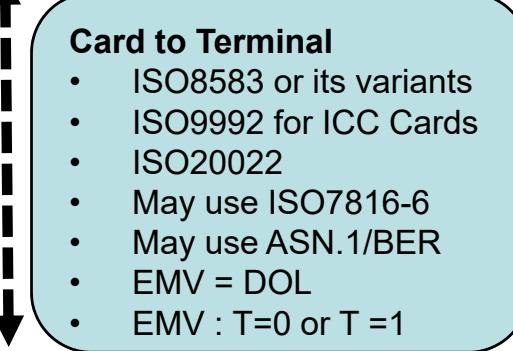
Communication



Terminal to Acquirer

- NDC/DDC
- ISO20022
- UK: Standard 70
- May use BASE64

NDC Example



Magstripe/ICC

A

Alfa·Bank

Acquirer

NPCI

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Network

Acquirer to Network and Network to Issuer

- ISO8583 or its variants
- ISO20022
- May use ISO7816-6
- May use ASN.1/BER
- May use BASE64

**DELTA
BANK**

Issuer

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

OSI networking and system aspects – Abstract Syntax Notation One (ASN.1)

Information technology – ASN.1 encoding rules:
Specification of Basic Encoding Rules (BER),
Canonical Encoding Rules (CER) and
Distinguished Encoding Rules (DER)



EMV AND NON-EMV ONLINE TRANSACTION PROCESSING

On us transaction



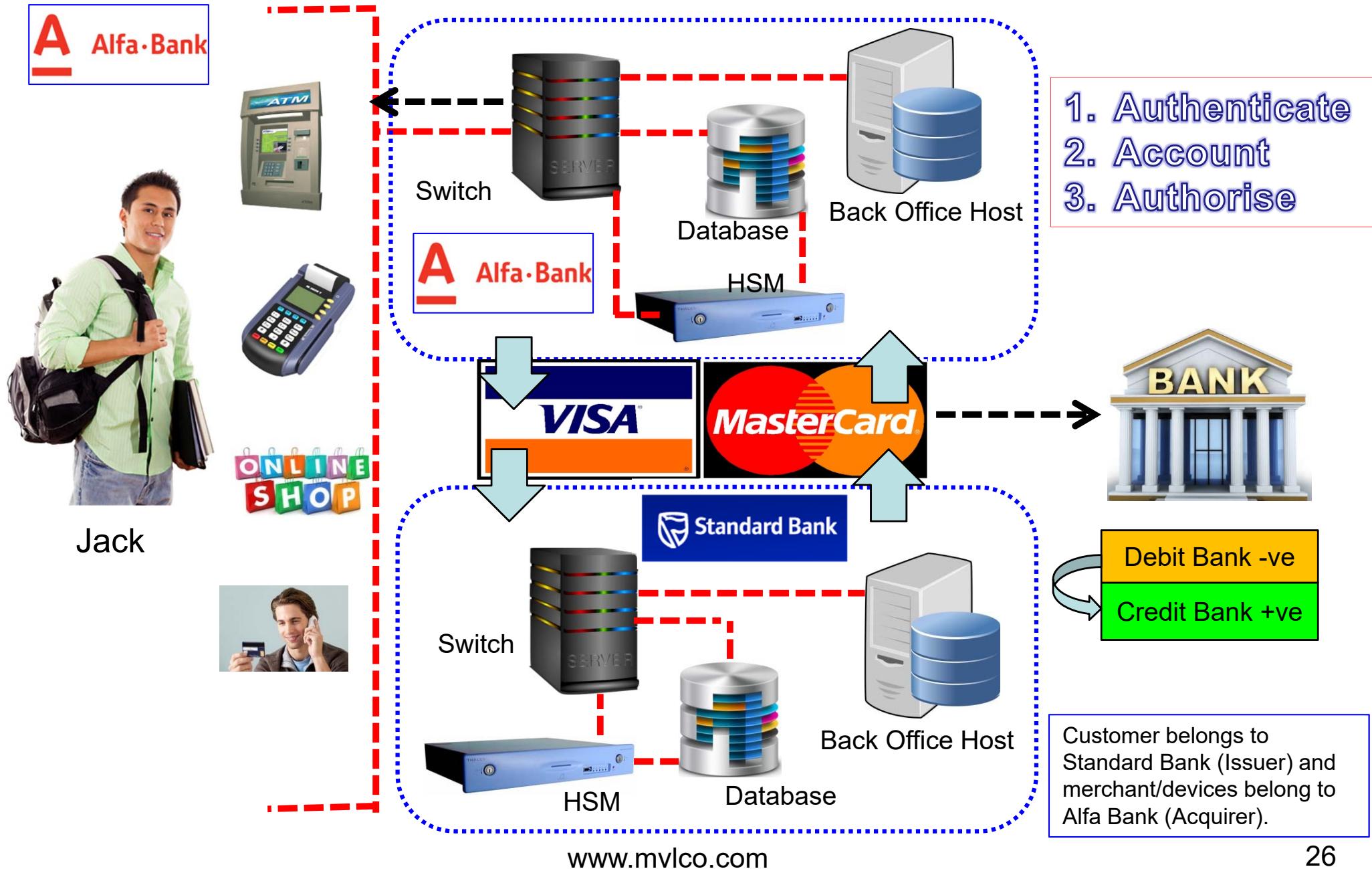
Jack



1. Authenticate
2. Account
3. Authorise

Customer and merchant/devices belong to the same bank.

Off us transaction





EMV 1

AAC	Application Authentication Cryptogram
AID	Application Identifier
ARC	Authorization Response Code
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
CAM	Card Authentication Method
CDA	Combined Dynamic Data Authentication
CVM	Cardholder Verification Method
DDA	Dynamic Data Authentication
IAC	Issuer Action Codes
ICC	Integrated Chip Card
SDA	Static Data Authentication
SVC	Service Code
TAC	Terminal Action Code
TC	Transaction Certificate
TVR	Terminal Verification Result



EVM transaction process

Snapshot (1)

- **Resetting the card**
 - Cold reset
 - Warm reset
- **Answer to Reset (ATR)**
 - Bit order : direct/inverse convention
 - Protocol : T=0 (Character frameset) or T=1 (Block frameset)
- **Application selection**
 - Payment System Environment (PSE) selection method
 - Application Identifier (AIDs) method
 - Build candidate list
 - Final selection
- **Initiate application process**
 - PDOL/Application Interchange Profile (AIP) / Application File Locator (AFL)
- **Read application data**
 - Read all data from AFL
 - Data authentication : SDA/DDA/CDA : Offline data authentication

AID List

EVM transaction process

Snapshot (2)

- **Processing restrictions**
 - Application version number
 - Application usage control
 - Application effective/expiration dates checking
- **Cardholder verification methods (CVM)**
 - Offline PIN verification
 - Online PIN verification
 - Signature
 - Combined CVM
 - No CVM required
- **Terminal risk management**
 - Terminal floor limit checking : Check log for same PAN, add recent entry, if any
 - Random transaction selection
 - Random selection : certain percentage below floor limit are sent online
 - Biased random selection : formula used to determine whether a transaction is to be sent online
 - Velocity checking :
 - Lower Consecutive Offline Limit/Upper Consecutive Offline Limit (LCOL/UCOL)
 - Lower cumulative offline transaction amount (LCOTA)/ Upper cumulative offline transaction amount (UCOTA)

EVM transaction process

Snapshot (3)

- **Terminal action analysis**

- to whether the transaction should be approved offline, declined offline, or transmitted online
- Transaction verification results (TVR)
- The TVR is evaluated with :
 - Issuer action codes (IAC) : Stipulate conditions : Denial/Online/Default
 - Terminal action codes (TAC) : Stipulate conditions : Denial/Online/Default
- Generate AC (Authentication Cryptogram) :
 - Request for AAC/ARQC/TC
 - CDA request

- **Card action analysis**

- Details of card risk management algorithms within the ICC are specific to the issuer
- as a result of the risk management process, an ICC may decide to complete a transaction online or offline or reject the transaction
- The ICC may also decide that an advice message should be sent to the issuer to inform the issuer of an exceptional condition.
- Results : TC, AAC or ARQC

EVM transaction process

Snapshot (4)

- **Online processing (in case ARQC is issued by ICC)**
 - Data sent to issuer for online authorization
 - ARPC sent by issuer to terminal.
 - In authorization response, the issuer may send issuer authentication data to terminal
 - The terminal provides the Issuer Authentication Data to the ICC in the EXTERNAL AUTHENTICATE command
 - the ICC may respond with SW1 SW2 = '9000'
- **Issuer – to – ICC script processing**
 - An issuer may provide command scripts to be delivered to the ICC by the terminal to perform functions that are not necessarily relevant to the current transaction but are important for the continued functioning of the application in the ICC.
 - A script may contain Issuer Script Commands not known to the terminal, but the terminal shall deliver each command to the ICC individually according to this specification.

EVM transaction process

Snapshot (5)

- **Completion**

- The completion function closes processing of a transaction.
- The terminal always performs this function unless the transaction is terminated prematurely by error processing.
- The ICC indicates willingness to complete transaction processing by returning either a TC or an AAC to either the first or second GENERATE AC command issued by the terminal. If the terminal decides to go online, completion shall be done when the second GENERATE AC command is issued.

Your transaction was successful

Transaction ID

11155359

Amount

23.00 GBP

Description

tools

CartID/your reference

VT-01- 3453242



logout



help



go!

Make another transaction



AUTHENTICATION, ACCOUNTING, AUTHORISATION - AAA

Authentication

I  PIN

- **Card present transactions (Electronic)**
 - PIN/Offline verification/Online verification
 - Signature
 - NSDT : Near Sound Data Transfer
- **Card not present transactions**
 - Online transactions
 - CVV2
 - One Time Password (OTP) : On mobile/card generated
 - MasterCard SecureCode/Verified by VISA (VbV)
 - Remote chip authentication : MasterCard Chip Authentication Program (CAP) and VISA Dynamic Password Authentication (DPA)
 - VoicePay
 - Adaptive authentication
 - Phone transactions
 - Address Verification Service (AVS)
 - IVRS/TPIN verification



**MasterCard SecureCode
for Online Merchants**

*Building Consumer Confidence,
Extending Your Market Reach*



Dynamic passcode reader

Authorization

1. Cardholder presents a Visa card to pay for purchases. For card-absent transactions, the cardholder provides the merchant with the account number, expiration date, billing address, and CVV2.



2. Merchant swipes the card, enters the dollar amount, and transmits an authorization request to the merchant bank. For card-absent transactions, the account number and other information may be digitally or key-entered.



3. Merchant bank electronically sends the authorization request to VisaNet.



4. VisaNet passes on the request to the card issuer.



5. Card issuer approves or declines the transaction.



6. VisaNet forwards the card issuer's authorization response to the merchant bank.



7. Merchant bank forwards the response to the merchant.



8. Merchant receives the authorization response and completes the transaction accordingly.

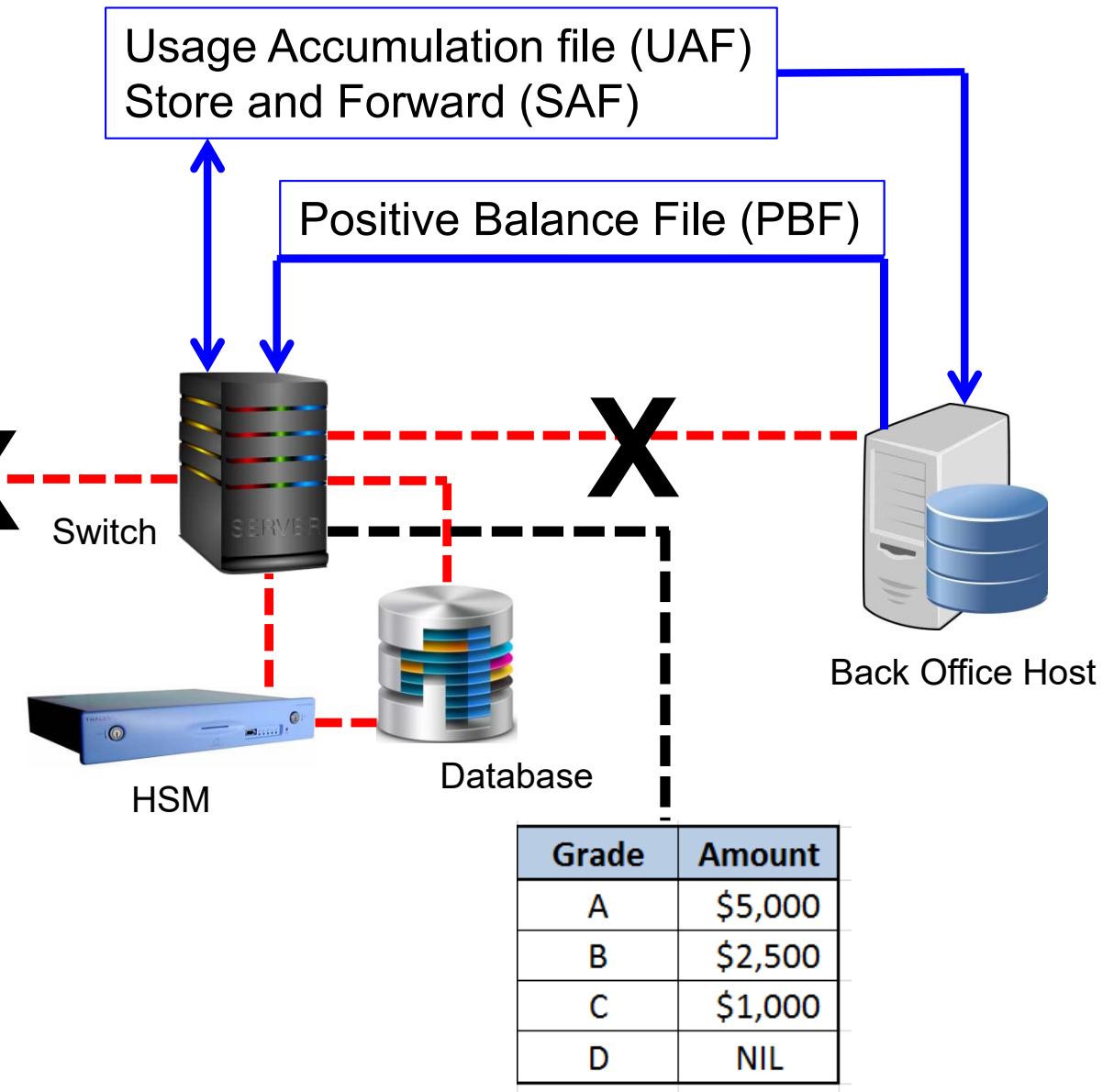


ACCOUNTING AND AUTHORISATION

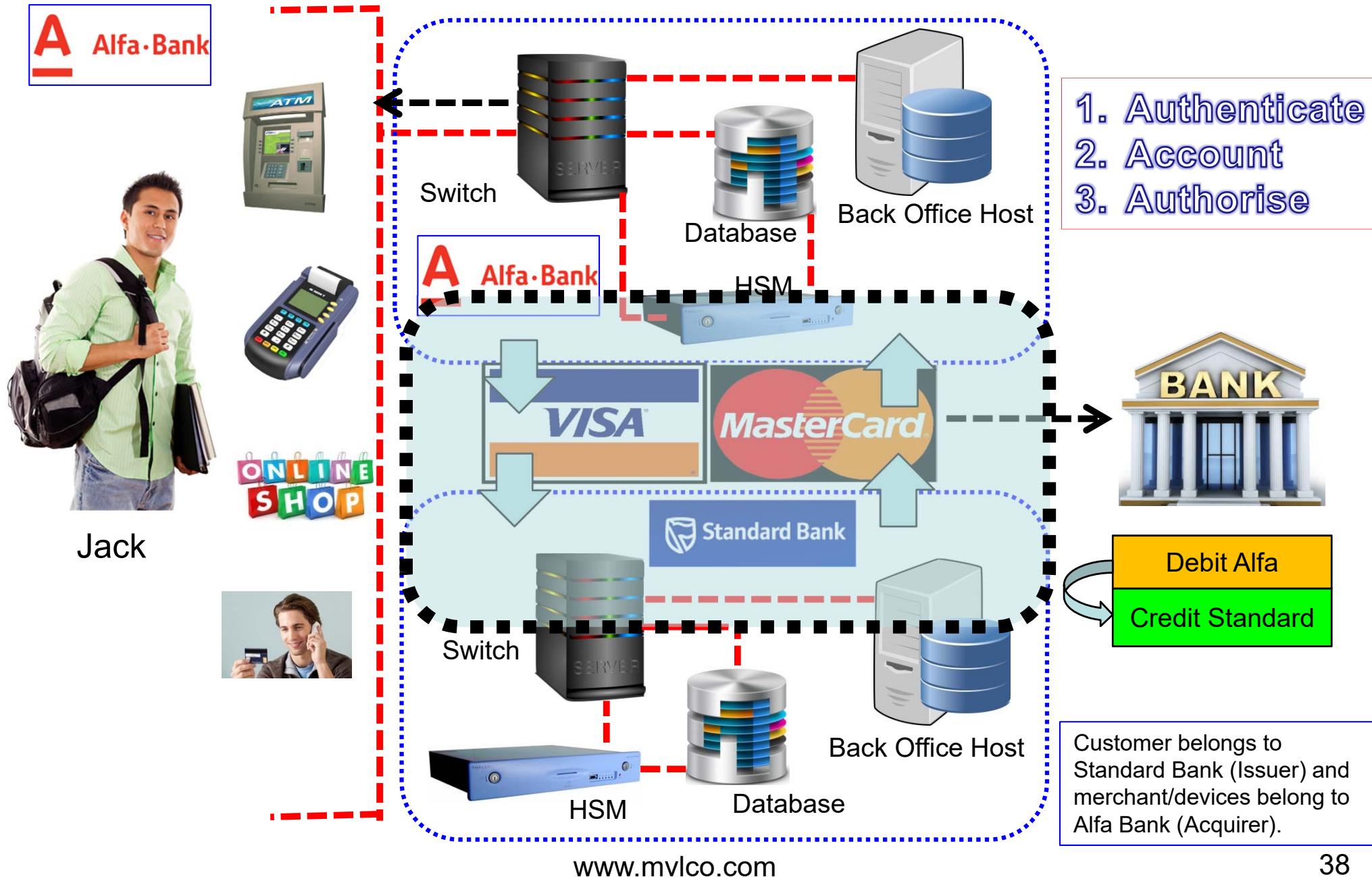
Electronic authorisation

- **Batch mode v/s. real time authorisation**
- **Online authorisation**
 - Positive/Negative/Usage
- **Offline authorisation**
 - Using PBF/SAF process
 - Card gradation
 - The Electronic Fall Back (EFB) facility using floor limit
 - IVRS Touchtone/voice authorisation
 - Floor limit – paper voucher
- **Stand-in processing – STIP**

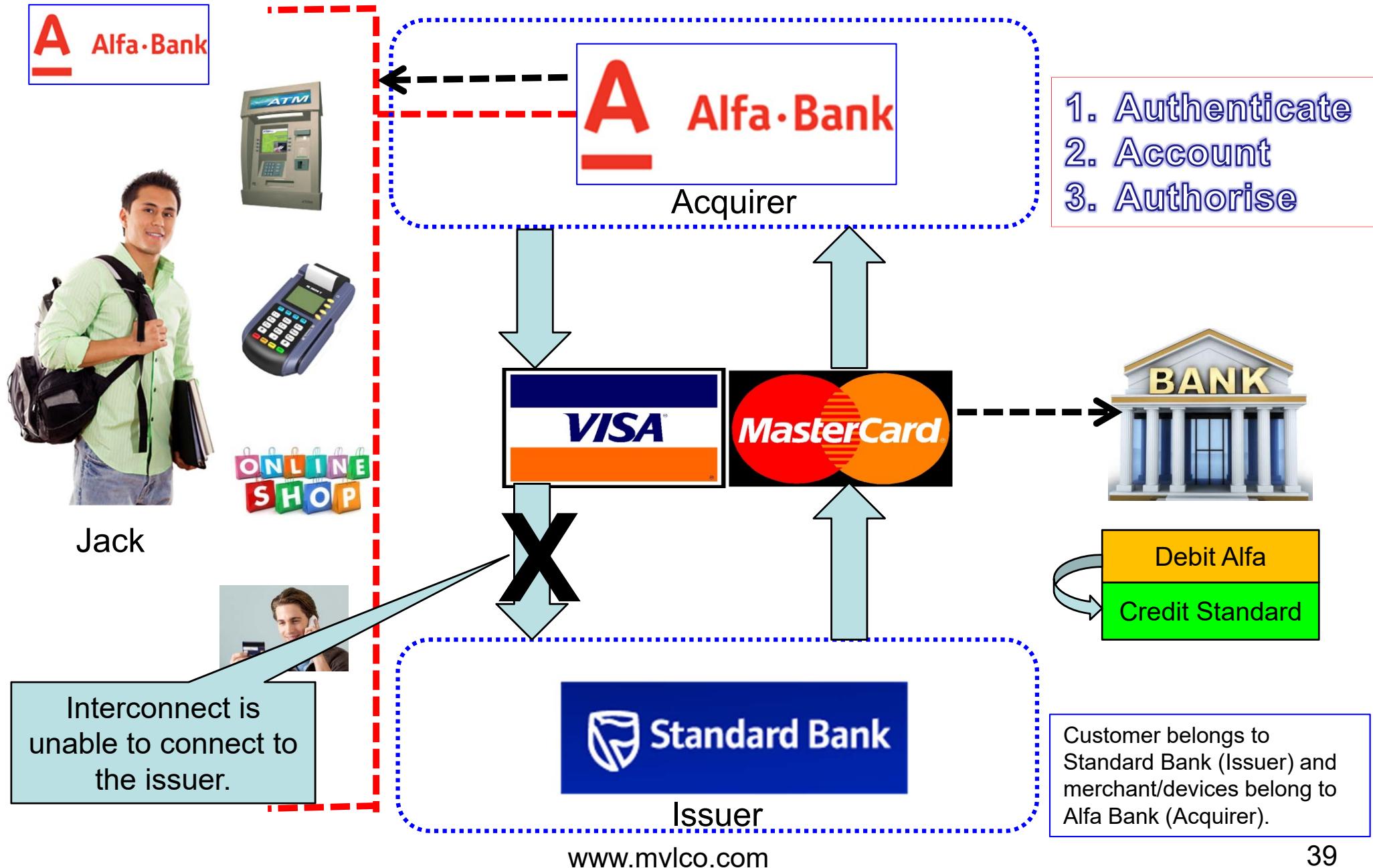
Recall ! On us transaction



Recall!! Off us transaction



Recall!! Off us transaction



Interconnect authorisation processes including STIP process (1)

- **Host Processor Authorization (STiP)**
 - The interconnect routes all transactions to issuer's system. If issuer's system is unavailable, interconnect can stand in and authorize transactions using limits and other criteria defined by the issuer.
- **Cooperative Authorization**
 - Working jointly with issuer's system , interconnect can pre-screen all or selected transactions based on limits or other criteria, including account balances, established by the issuer.
 - Transactions that pass pre-screening checks are then routed to issuer's system for final authorization.
 - Interconnect can also perform full stand-in authorization or authorize transactions below a floor limit you specify.

Interconnect authorisation processes including STIP process (2)

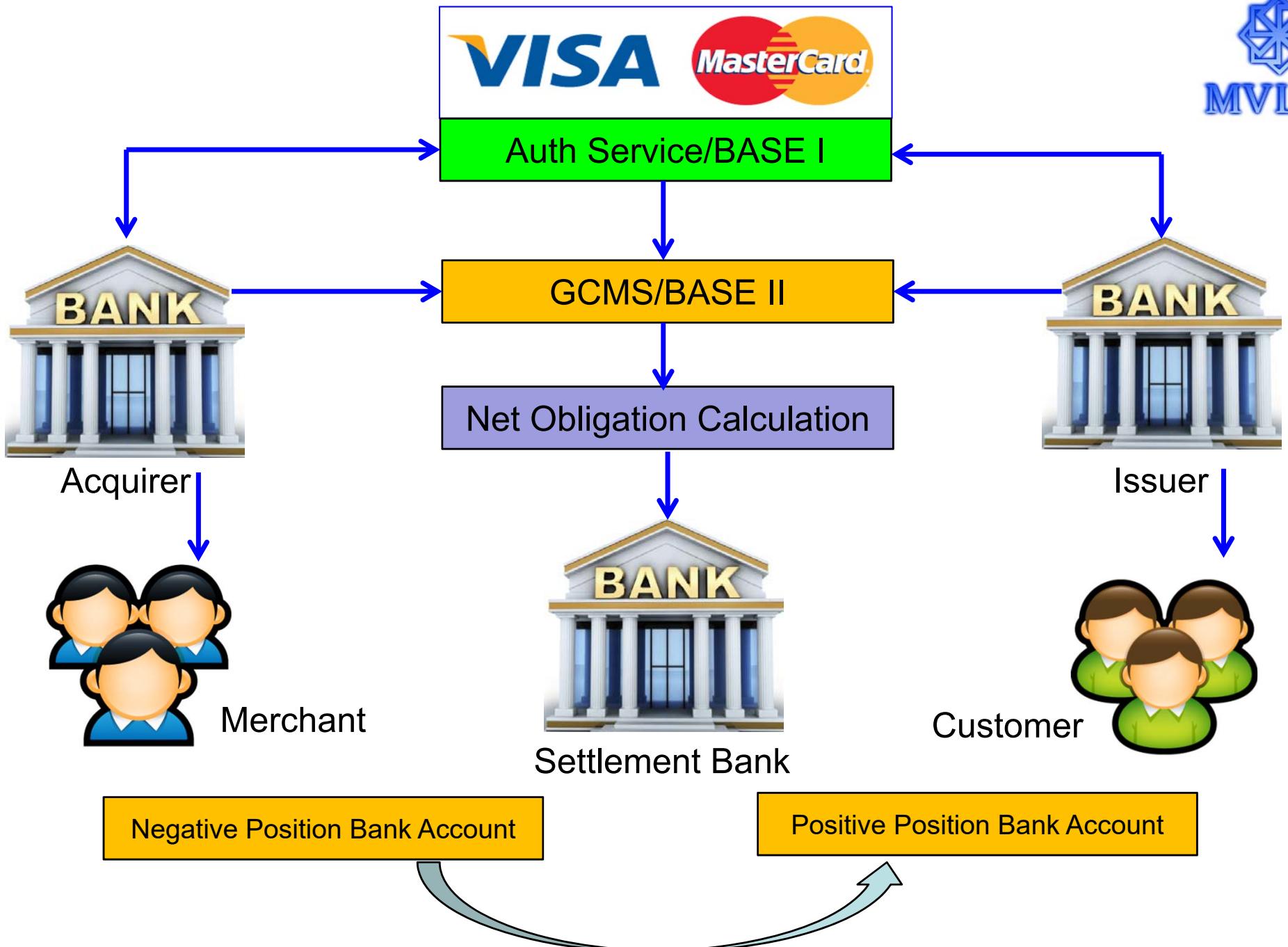
- **Stand-Alone Authorization**
 - Interconnect makes all authorization decisions using client-defined parameters, such as activity limits and account balances, without requiring a full-time online link to issuer's system. Interconnect creates and sends a batch-posting file to issuer's system at the end of each settlement day.
- **Prepaid Authorization**
 - Interconnects also support a turnkey prepaid solution. Interconnect routes the prepaid transaction to the Interconnect prepaid processing host system, which authorizes transactions and deducts the amount from the card balance.
 - Similar to the Stand-Alone Authorization option, the prepaid host stores and maintains all authorization decisions based on issuer specifications.



INTERBANK SETTLEMENT

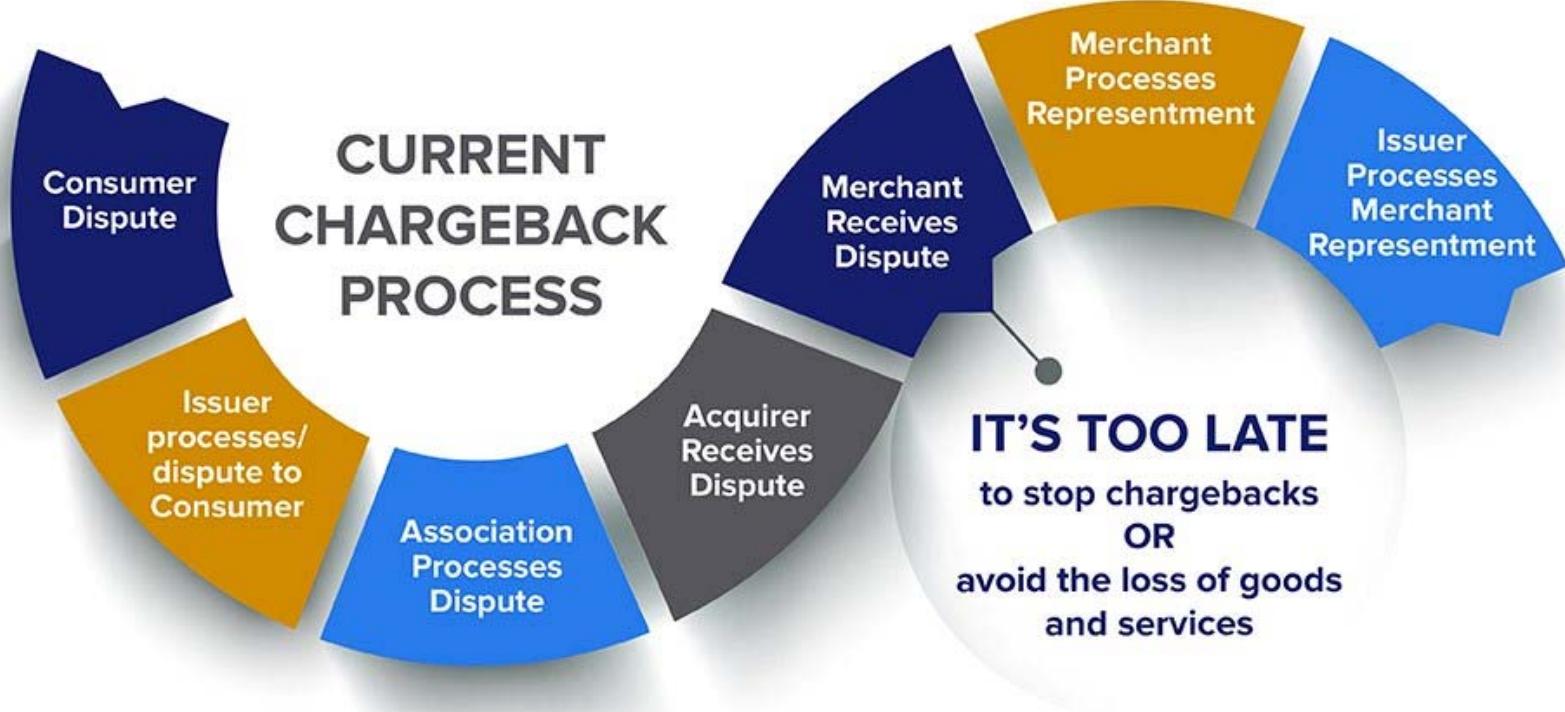
Interbank settlement

- There is only one settlement window, which is used for both dual-message and single-message transactions. When settlement is performed, it is done on an aggregate net basis. (VISA BASE I and BASE II – MasterCard Global Clearing Management System (GCMS))
- For issuing banks, most of their cardholders' activity is in the debit category; they are making purchases for which their bank will pay into settlement on the cardholders' behalf.
 - Exception : return of goods and chargebacks
- For acquiring banks, most of their merchants' activity will be credit transactions; i.e., they will generate an incoming flow of funds through the settlement process.
 - Exceptions : refunds, returns and chargebacks



VISA BASE I and BASE II

- There is only one settlement window, which is used for both dual-message and single-message transactions. When settlement is performed, it is done on an aggregate net basis.
- Visa's processing network is called the VisaNET Integrated Payment System (VIP). **VIP is comprised** of a number of different components including **an authorization system, called Base I**, and **a settlement system, called Base II**.
- Base I was created in 1976 by Bank of America's IT staff. **BASE stands for Bank of America System Engineering**. The system was given this name because prior to 1973, Visa was known as BankAmericard.



BILLING ERRORS AND CHARGEBACKS

Charge back

- A chargeback is the reversal of a charge on a card. This usually the result of the card holder disputing the charge.
- A consumer may initiate a chargeback by contacting their issuing bank, and filing a substantiated complaint regarding one or more debit items on their credit card statement.
- **Sample reasons:**
 - Double billing
 - Fraudulent billing
 - Improper or delayed credit for a cancelled transaction
 - Goods/services not delivered
 - Transaction declined but billed due to technical error

Transaction - Chargeback – Fund Flow

If a transaction is disputed, the fund flow starts moving back and forth !!

- Customer maybe given temporary credit for disputed transaction
- Issuer debits Acquirer through association.
- Acquirer may debit merchant account held by them.
- If merchant proves he is not at fault, again merchant account is credited by Acquirer.
- Acquirer then debits Issuer for the same transaction
- Issuer reverses customer credit and debits customer again for the transaction.



Process of chargeback

- When a chargeback right applies, the issuer sends the transaction back to the acquirer and charges back the dollar amount of the disputed sale.
- The acquirer then researches the transaction. If the chargeback is valid, the acquirer deducts the amount of the chargeback from the merchant account and informs the merchant.
- Under certain circumstances, a merchant may **re-present** the chargeback to its acquirer.
- If the merchant cannot remedy the chargeback, it is the merchant's loss. If there are no funds in the merchant's account to cover the chargeback amount, the acquirer must cover the loss.
- Copy request:
 - When a card issuer sends a copy request to an acquirer, the bank has 30 days from the date it receives the request to send a copy of the sales receipt back to the card issuer.

Arbitration process

- If the card issuer disputes a representation from the acquirer, the card issuer may file for arbitration with Visa.
- In arbitration, Visa decides which party is responsible for the disputed transaction.
- In most cases, Visa's decision is final and must be accepted by both the card issuer and the acquirer.
- During arbitration, Visa reviews all information/documentation submitted by both parties to determine who has final liability for the transaction.

Chargeback monitoring program

- The Merchant Chargeback Monitoring Program (MCMP) monitors chargeback rates for all acquirers and merchants on a monthly basis. If a merchant meets or exceeds specified chargeback thresholds, its acquirer is notified in writing.
- First notification of excessive chargebacks for a specific merchant is considered a warning.
- If actions are not taken within an appropriate period of time to return chargeback rates to acceptable levels, Visa may impose financial penalties on acquirers that fail to reduce excessive merchant chargeback rates.

HRCMP

- The High Risk Chargeback Monitoring Program (HRCMP) is specifically targeted at reducing excessive chargebacks by high-risk merchants.
- As defined by Visa, high-risk merchants include direct marketers, travel services, outbound telemarketers, inbound teleservices, and betting establishments.
- HRCMP applies to all high-risk merchants that meet or exceed specified chargeback thresholds.
- Under HRCMP, there is no warning period and fees may be assessed to the acquirer immediately if a merchant has an excessive chargeback rate.

Global Merchant Chargeback Monitoring Program

- **Global Merchant Chargeback Monitoring Program - Merchant Disqualification**
- Visa may disqualify a Merchant that has been placed in the Global Merchant Chargeback Monitoring Program from participation in the Visa Program if the Merchant meets or exceeds the specified Chargeback ratio threshold of 2% without an effective Chargeback reduction plan, and 2 of the following levels of Chargeback activity are reached:
 - Merchant's Chargeback ratio is 2 or more times the specified Chargeback ratio in a single month
 - Merchant is assessed fees for 3,000 or more Chargebacks in a single month
 - Merchant is assessed US \$1 million or more in Global Merchant Chargeback Monitoring Program fees

ID#: 081010-010410-0002445

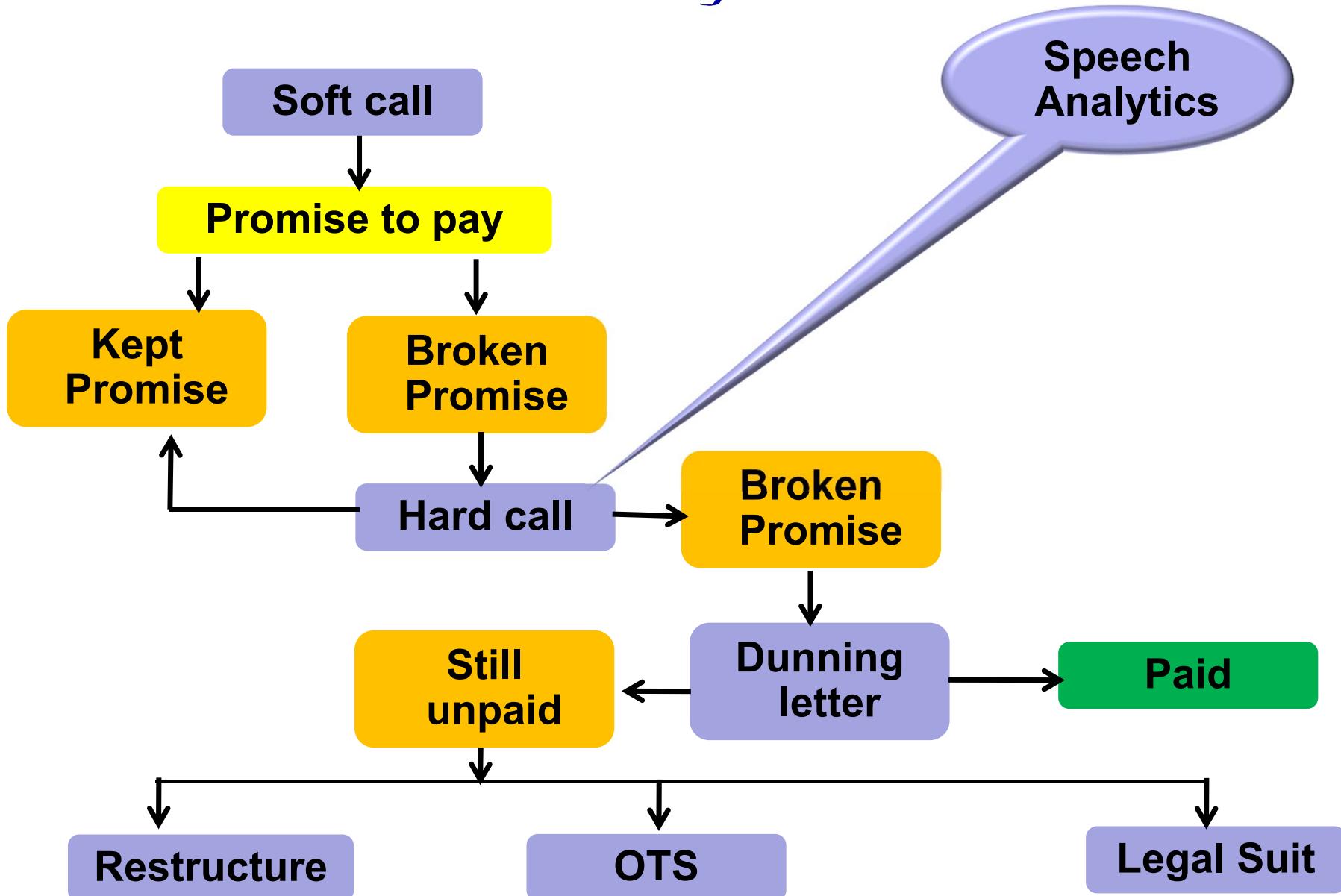
Termination of Merchant Agreement

After verifying that Visa has prohibited a Merchant or Sponsored Merchant from participating in the Visa or Visa Electron Program, an Acquirer must terminate the Merchant Agreement no later than the date specified by Visa.



COLLECTION AND RECOVERY

Collection/recovery



Steps in the Bank Reconciliation Process

Gather information

Identify discrepancies

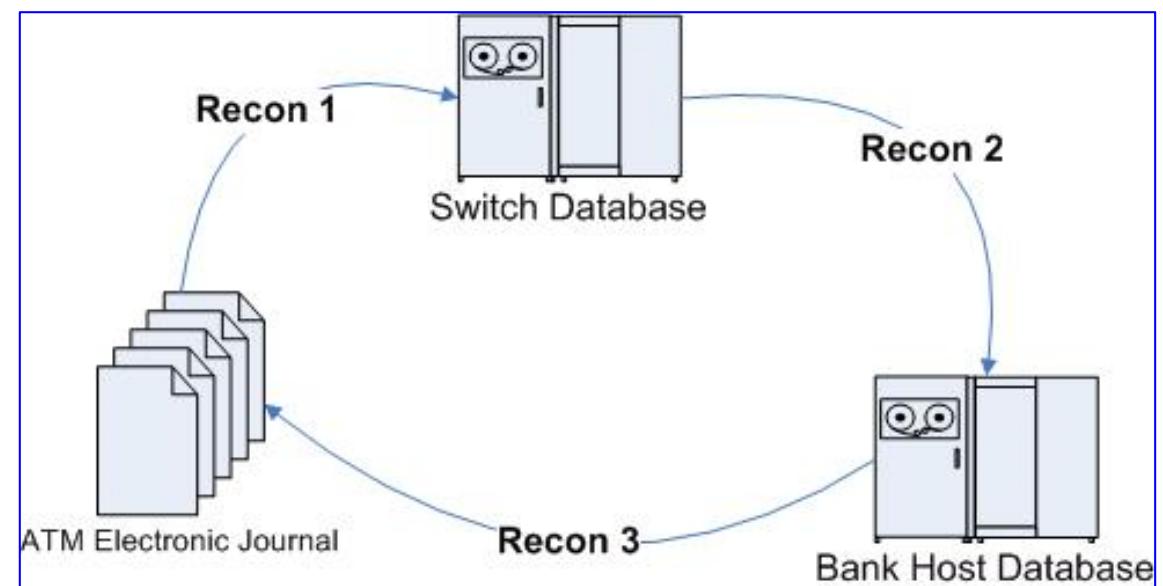
Update accounting records

Prepare a bank reconciliation statement

RECONCILIATION

Reconciliations

- With customers
- With merchants
- With inter-change
- With settlement bank
- Cash reconciliation



Card Payment Systems

Module 5

Card Frauds, PCI DSS and EMV Standards

MVL Consulting Private Limited
www.mvlco.com

Credit card frauds

- Credit card fraudsters employ a large number of modus operandi to commit fraud.
- **Card related frauds**
 - Application fraud
 - Lost/stolen cards
 - Account takeover
 - Fake and counterfeit cards
 - Skimming/shimming
- **Merchant related frauds**
 - Merchant collusion/selling customer data
 - Triangulation – creating websites to capture customer data by offering large discounts
 - Site cloning/fake websites

Card Frauds

Type	Occurs when...	Additional remarks	Detection & Prevention
<i>Application fraud</i>	Personal acquaintance or unknown individual gains access to victim's SSN, DoB, mailing info ; applies for credit card; uses the received card without victim's knowledge	Familiar Vs unfamiliar	Through investigation
<i>Lost and stolen credit cards</i>	Credit card is lost or stolen	Most common form Direct access to victim's account May gain access to personal info and can apply for other cards	Generally, quickly recognized Cardholders covered if loss or theft is promptly reported
<i>Non-receipt (mail intercept) fraud</i>	Individual's mail is intercepted by criminal		Card activation process
<i>Counterfeit cards</i>	Criminal manufactures false card when in possession of valid card number	Skimming devices – access and store data from magnetic stripe for later use	Real time terminal authorizations
<i>Account takeover</i>	Criminal obtains enough information about an individual to represent the victim to issuer bank	First step – request change of address Second step – Report lost / stolen card and get the new card issued	Verification by phone and / or duplicate mailings to both addresses
<i>Bust-out-fraud</i>	True customer gradually builds up credit on multiple credit cards and then bursts-out	Very large loss consequences Difficulty in separating these criminals from the general base of	Closure of account if sudden deviation from model behavior

DATA BREACH AND HACKING

Carding

- **Heartland Payment Systems USA**
 - Major payments processor
- Albert Gonzalez & accomplices **hacked 130 million cards over 6 months**
 - Caught - pleaded guilty
- Fed. Reserve Bank Philadelphia publication
 - *Heartland Payment Systems:
Lessons Learned from a Data Breach*



FRAUD PREVENTION

Tools for fraud prevention/detection

- Tokenisation
- Simple rule system
- Fraud scoring/predictive tools
- Artificial intelligence
 - Neural networks
 - Regression analysis
 - Decision trees
 - Clustering
 - Logistic regression
- Decision trees and neural networks build classification rules and other mechanisms for detecting fraud.
- Clustering can indicate what types of groupings in a given population (based on a number of inputs) are more at risk for exhibiting fraud.



PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI DSS

Build and maintain a secure network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly monitor and test networks

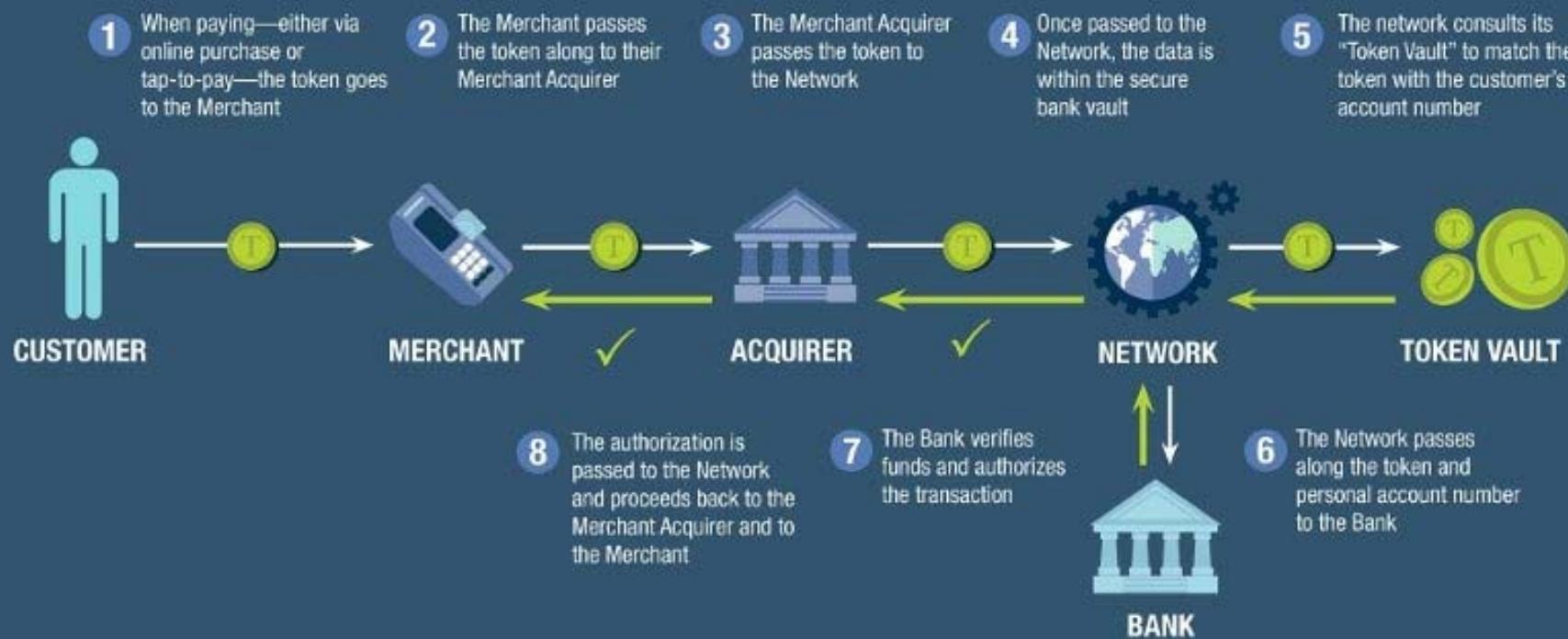
Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an information security policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

HOW DOES A TOKENIZED TRANSACTION WORK?



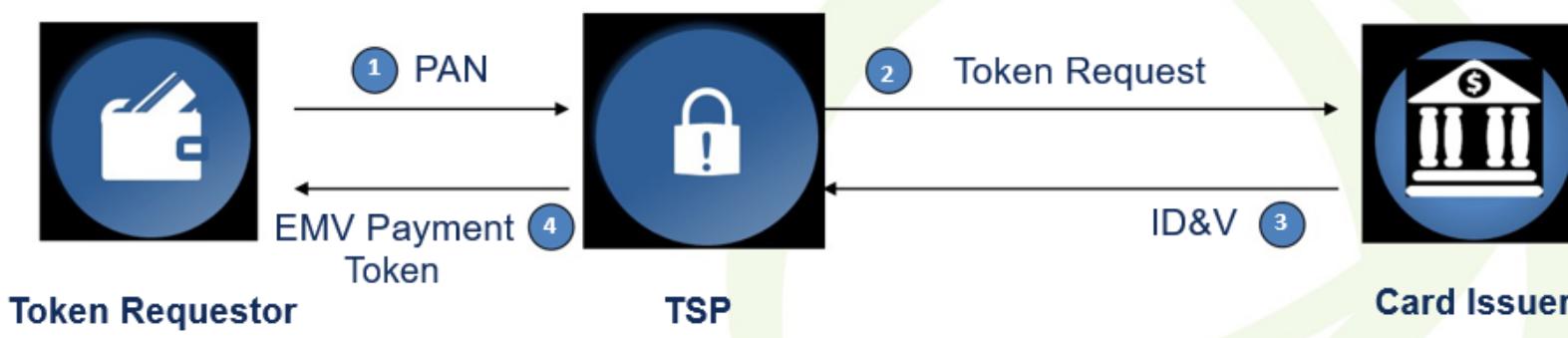
TOKENISATION

Token issue process

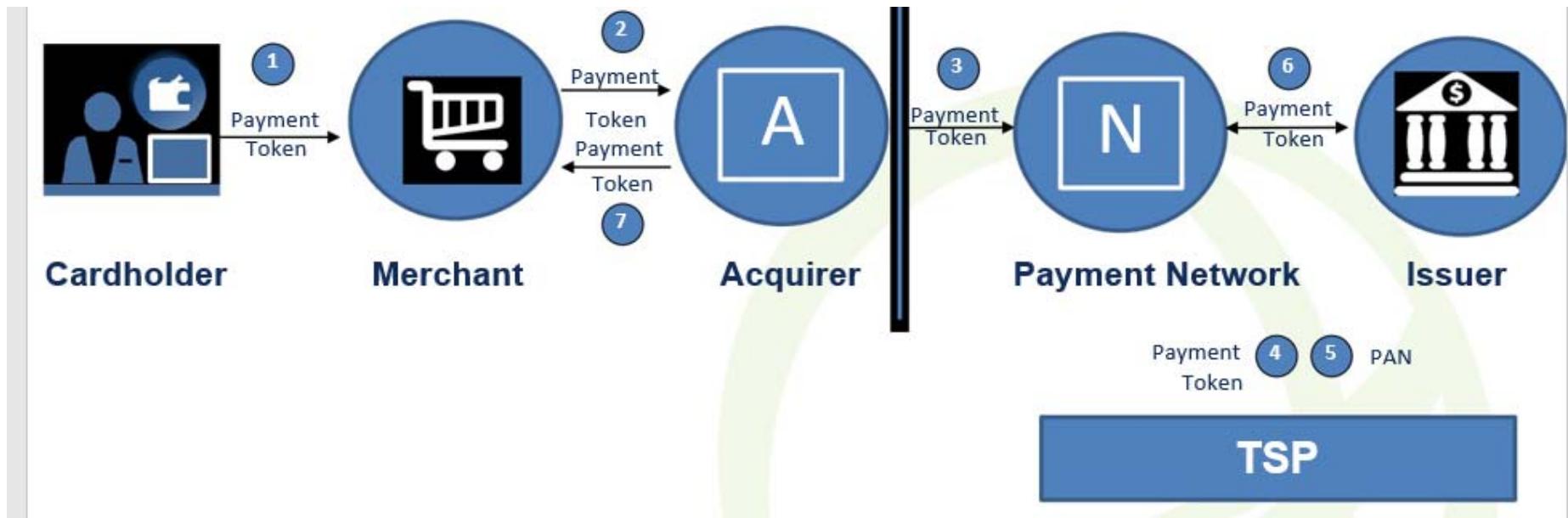
EMV Payment Token requests are made to a TSP. The token requestor, TSP and card issuer can all participate in ID&V. A token requestor can be a wallet, merchant, etc.

Process:

1. Token requestor sends a cardholder PAN to the TSP (a request)
2. As part of the token request process, the TSP alerts the card issuer that ID&V is needed
3. Card issuer (or TSP on issuer's behalf) performs ID&V and passes results to the token vault (Binding)
4. TSP passes the registered EMV Payment Token to the token requestor



Token usage process



- (1) Cardholder initiates a purchase with a payment instrument i.e. EMV Payment Token.
- (2) and (3) Payment Token flows through the merchant and acquirer as if it were a PAN
- (4) and (5) Payment token is de-tokenised into a PAN by the TSP; card issuer makes authorization decision and returns PAN to TSP
- (6) and (7) TSP re-tokenises the PAN and the authorisation response flows back through the acquirer to the merchant

Thank You !

