Card Payment Systems

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

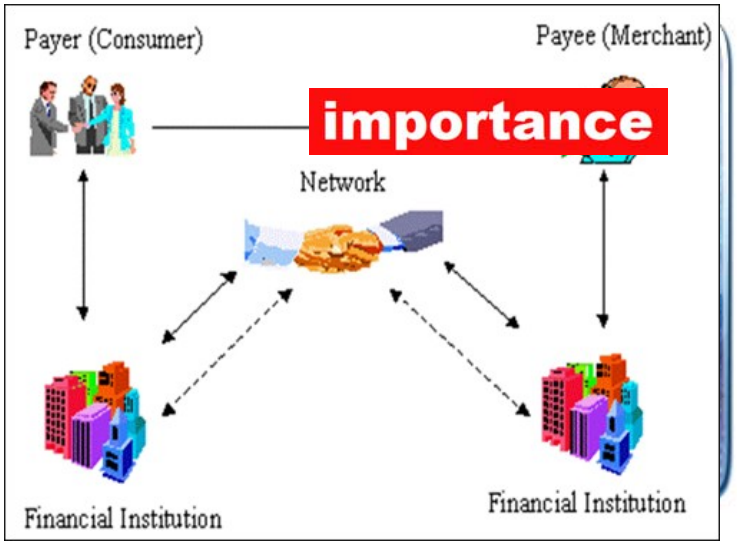
www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *Brief history of card payment systems*
2. *Players in payment card industry and their roles*
3. *Card schemes and types of cards*
4. *Types of permitted transactions*

Key elements of payment

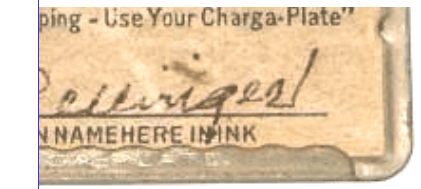


- **Message**
  - instructions or request to pay
- **Clearing**
  - message processing, may involve netting
- **Settlement**
  - exchange of value between parties

- **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
- **1949** : Frank X. McNamara and Ralph Sch
- **1950** : Diners Club was founded by Frank X. McNamara and Ralph Schneider
- **1951** : The Fran
  and introduced
- **1958** : Bank of A
- asterCard was born
  ge to compete with E
- United Kingdom lau
  .

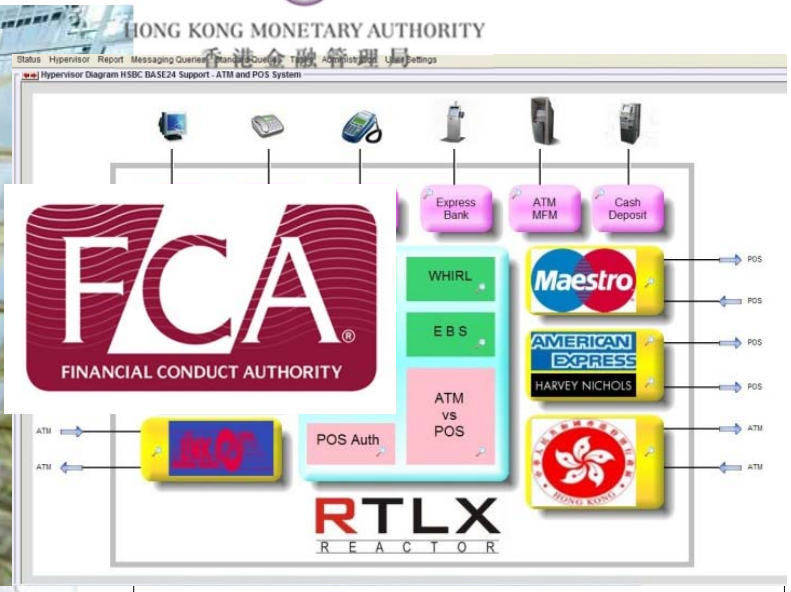


Players in Payment Card Industry (PCI)

MVLCO

Cardholder/ Customer

Customer associated with the Primary Account Number



BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

FCA
FINANCIAL CONDUCT AUTHORITY

connectivity, clearing and settlement services among banks. Aggregators e.g. Paytm

Service Providers

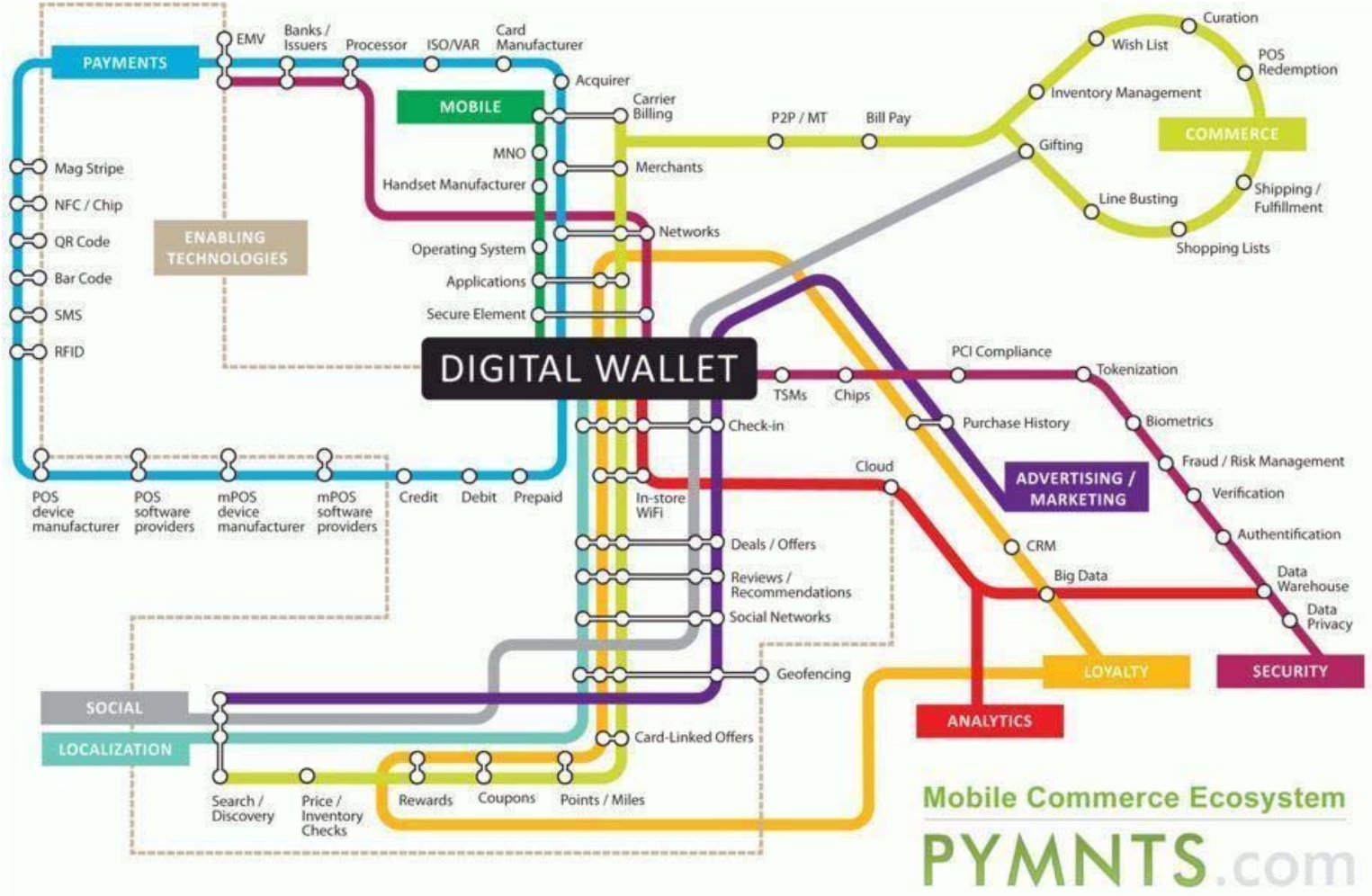
Providing networking services, ATM maintenance services, cash vault and cash management services to financial institutions.

Manufactures and D

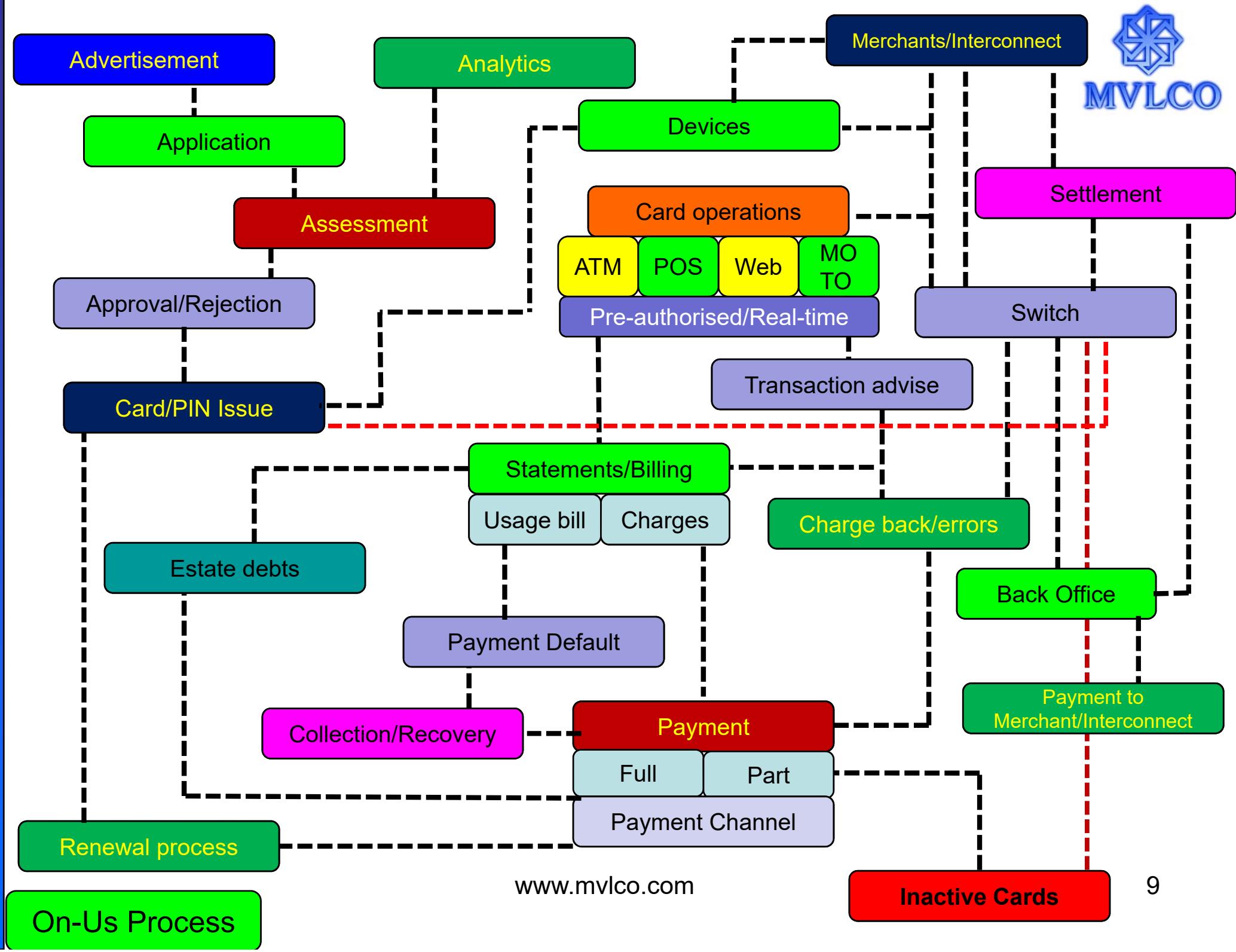
Card devi manu applica frau

developers

Regulators



CREDIT CARDS (BROAD LEVEL) LIFECYCLE EVENTS


Advertisement
Analytics
Merchants/Interconnect
MVLCO
Application
Devices
Settlement
Assessment
Card operations
ATM
POS
Web
MO TO
Approval/Rejection
Pre-authorised/Real-time
Switch
Transaction advise
Card/PIN Issue
Statements/Billing
Usage bill
Charges
Charge back/errors
Estate debts
Back Office
Payment Default
Payment to Merchant/Interconnect
Collection/Recovery
Payment
Full
Part
Payment Channel
Renewal process
Inactive Cards
On-Us Process

MVLCO

SCHEMES AND TYPES OF CARDS - PRODUCTS

Card schemes

- T
- F

Same
ty

DISCOVER

Diners Club INTERNATIONAL

AMERICAN EXPRESS

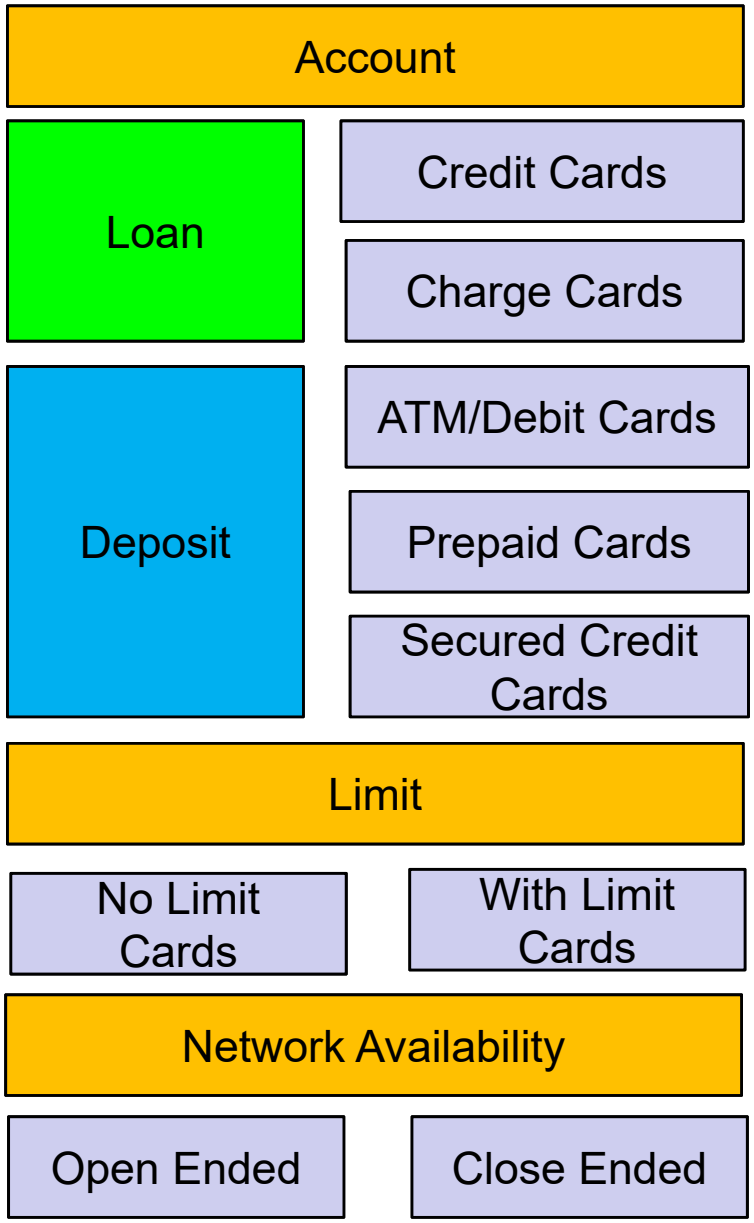
er

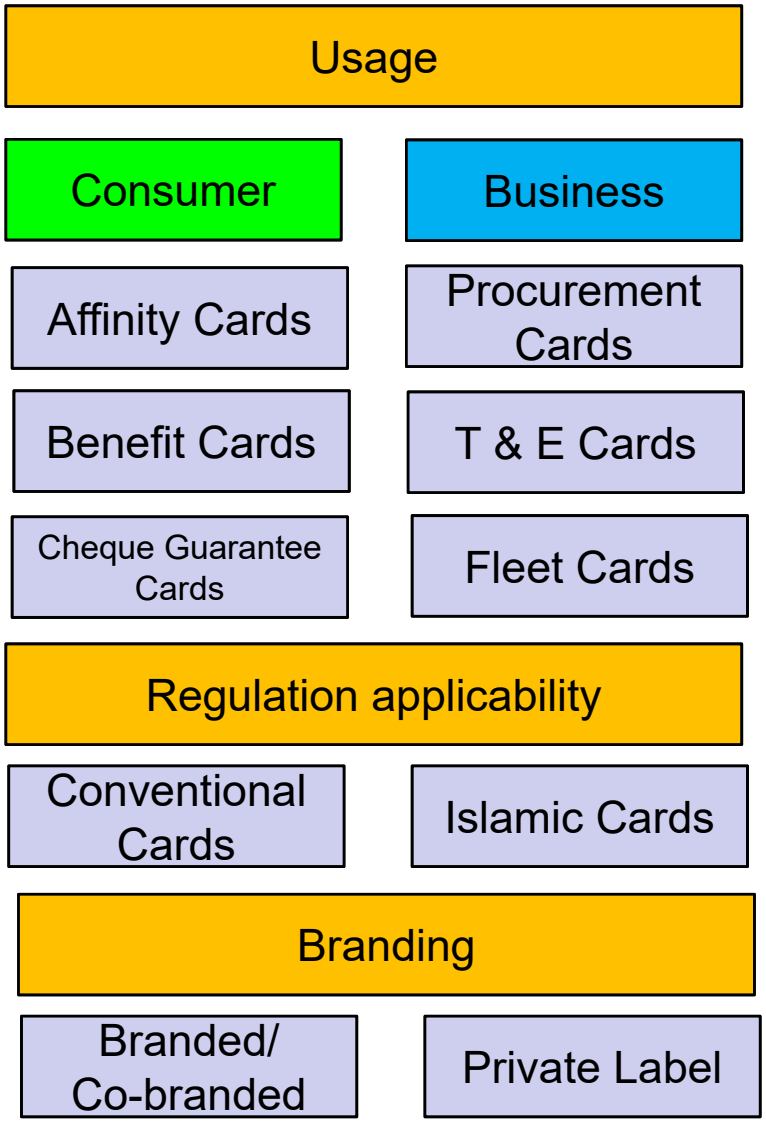
The Four Party System

These companies make money from transaction fees and volume fees.

These companies **DO NOT** issue cards or extend credit.

Card classification





Various card brands

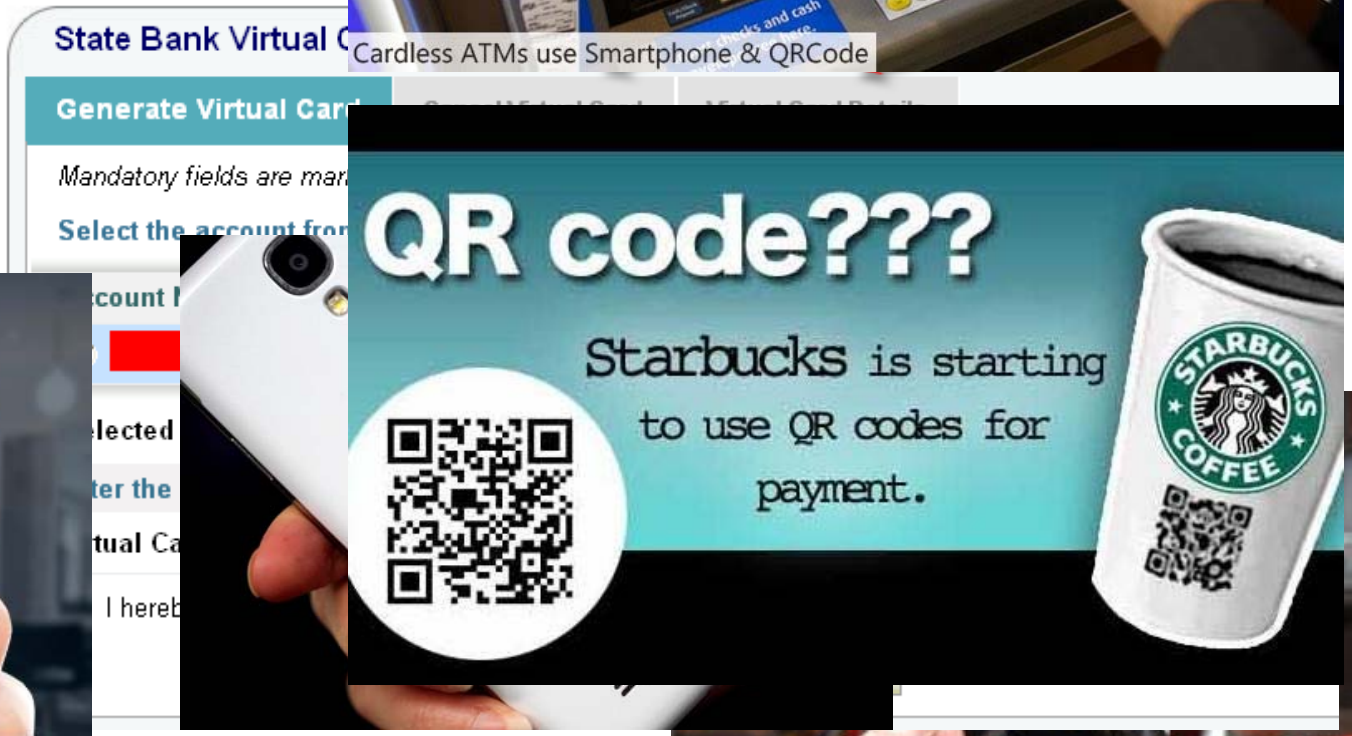
- Visa
- Visa Electron
- Visa Paywave
- MasterCard
- MasterCard Electronic
- MasterCard Maestro
- American Express
- Diners Club
- JCB
- Discover
- Rupay
- Many more….

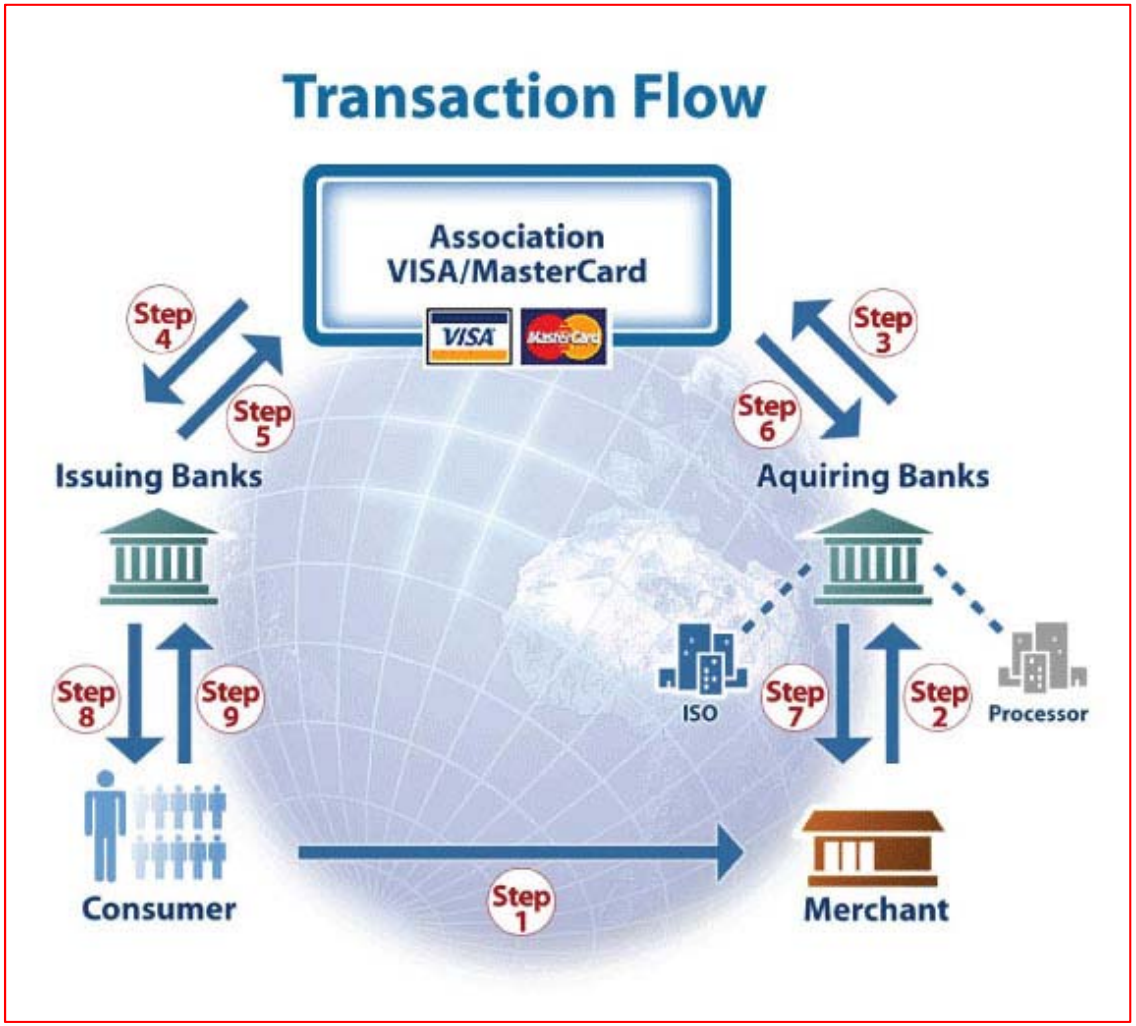
Card classification

ISO 7810/ISO 7816

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

Cardless ATMs use Smartphone & QRCode





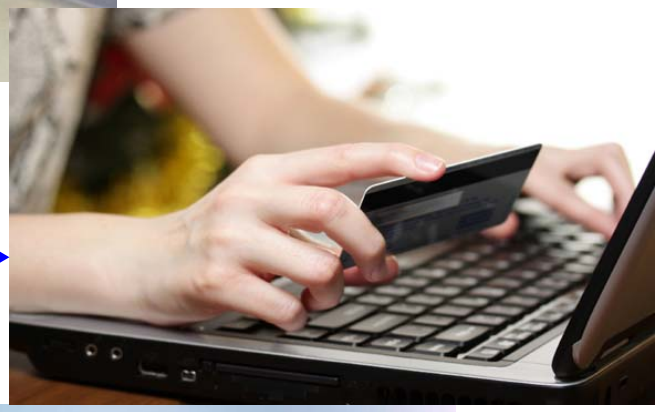
PERMITTED TRANSACTIONS

Permitted transactions

- Cash Withdrawal from ATM
  - With card
  - Cardless
- Purchase of Merchandise
- Cash Out
- Internet Commerce
- Utility Payments
- Bill Payments
- Balance Transfers
- Fund Transfers
- Loan against Cards
- EMI transactions
- Cash advance cheque

Card Present (CP)

Card Not Present (CNP)



MVLCO

TRANSACTION PROCESS OVERVIEW

On us transaction

Jack

Switch

Back Office Host

HSM

Database

Standard Bank

1. Authenticate
2. Account
3. Authorise

Customer and merchant/devices belong to the same bank.

Off us transaction

MVLCO

Alfa-Bank

Jack

Switch

Database

Back Office Host

Alfa-Bank

HSM

VISA

MasterCard

Standard Bank

Switch

Database

Back Office Host

HSM

1. Authenticate
2. Account
3. Authorise

Debit Alfa

Credit Standard

Customer belongs to Standard Bank (Issuer) and merchant/devices belong to Alfa Bank (Acquirer).

Card Payment Systems

Module 2
Understanding Card and PIN

MVL Consulting Private Limited

www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *Structure of cards*
2. *PIN*

Card front

Individual Account Identifier Number

Issuer Identifier Number (IIN)

7. Embedded µChip

Major Industry Identifier (MII)

8. Issue Date (Valid From) MM/YY

Bank Identification Number (BIN) is 1st 4-digits of CC No. BIN is now replaced by IIN.

1. Logo or Symbol of a credit card Issuing Entity.

2. Credit Card Payment Processor's Logo.

3. Hologram (3D Image)

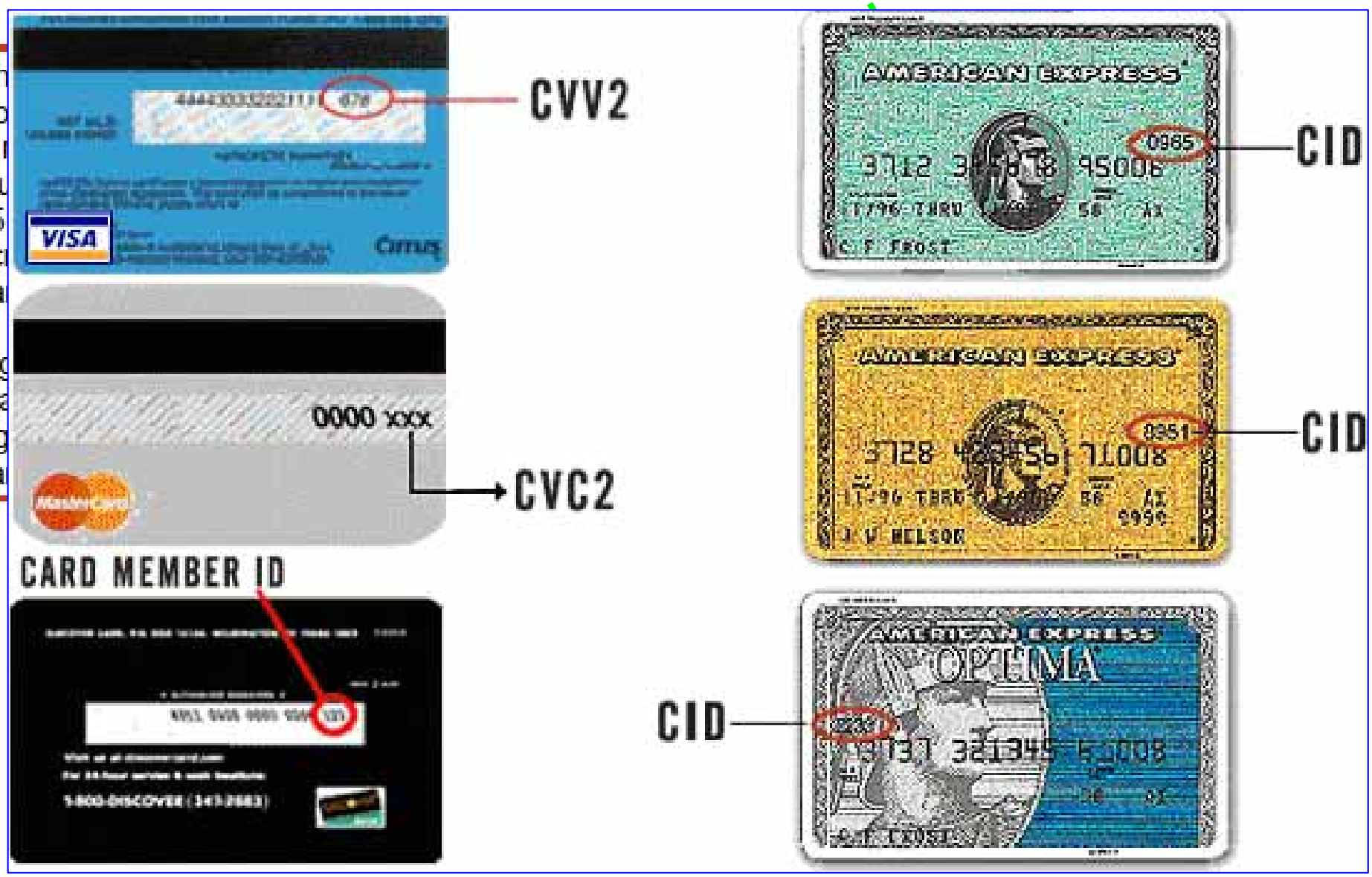
Check Digit or Checksum

5. Expiration (Last) Date (Valid Thru) i.e. (Valid Until) Uses MM / YY date format.

4. An Embossed or Printed 16-digits Credit Card Number grouped in four sets with 4-digits in each set and follows an ISO/IEC 7812-1 card numbering system.

6. Cardholder Name has first and last name of an individual OR registered name of a company / firm / organization / institution

Card backside



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

MVLCO

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)

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

Card Payment Systems

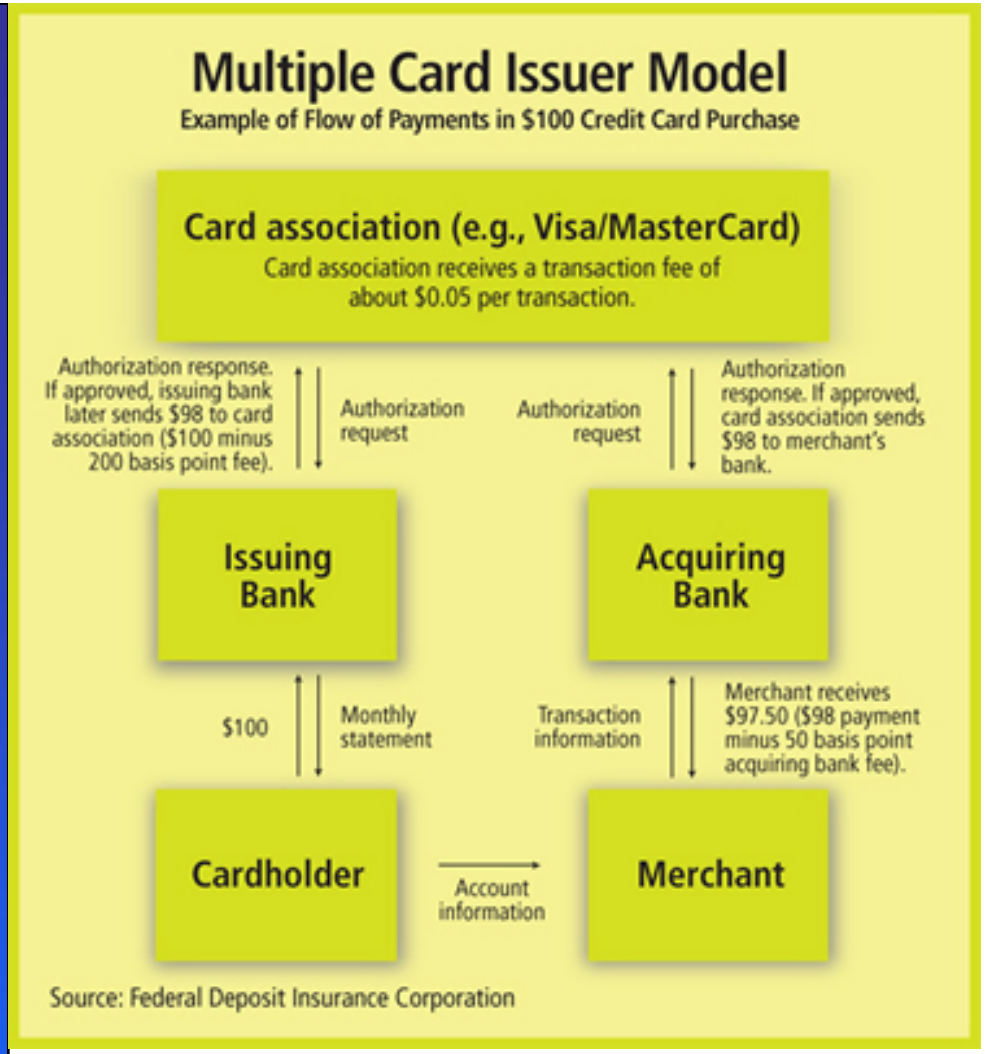
Module 3
Before Starting Card Operations

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 ISSUANCE PROCESS

Issuance process in brief

- Advertisement
- Application
- De-dupe – internal/external
- Document verification
- Customer contact program (CCP)
- Credit assessment (using financials, scores and results of CCP)
- Limit sanction and program/scheme attachment
- Card production
  - Tipping
  - **Personalisation**
- PIN generation
- Upload data in server/switch
- Card and PIN handover to customer

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

Alfa-Bank

Acquirer

NPCI भारतीय राष्ट्रीय भुगतान निगम NATIONAL PAYMENTS CORPORATION OF INDIA

Network

Card to Terminal
- ISO8583 or its variants
- ISO9992 for ICC Cards
- ISO20022
- May use ISO7816-6
- May use ASN.1/BER
- EMV = DOL
- EMV : T=0 or T =1

Acquirer to Network and Network to Issuer
- ISO8583 or its variants
- ISO20022
- May use ISO7816-6
- May use ASN.1/BER
- May use BASE64

Magstripe/ICC

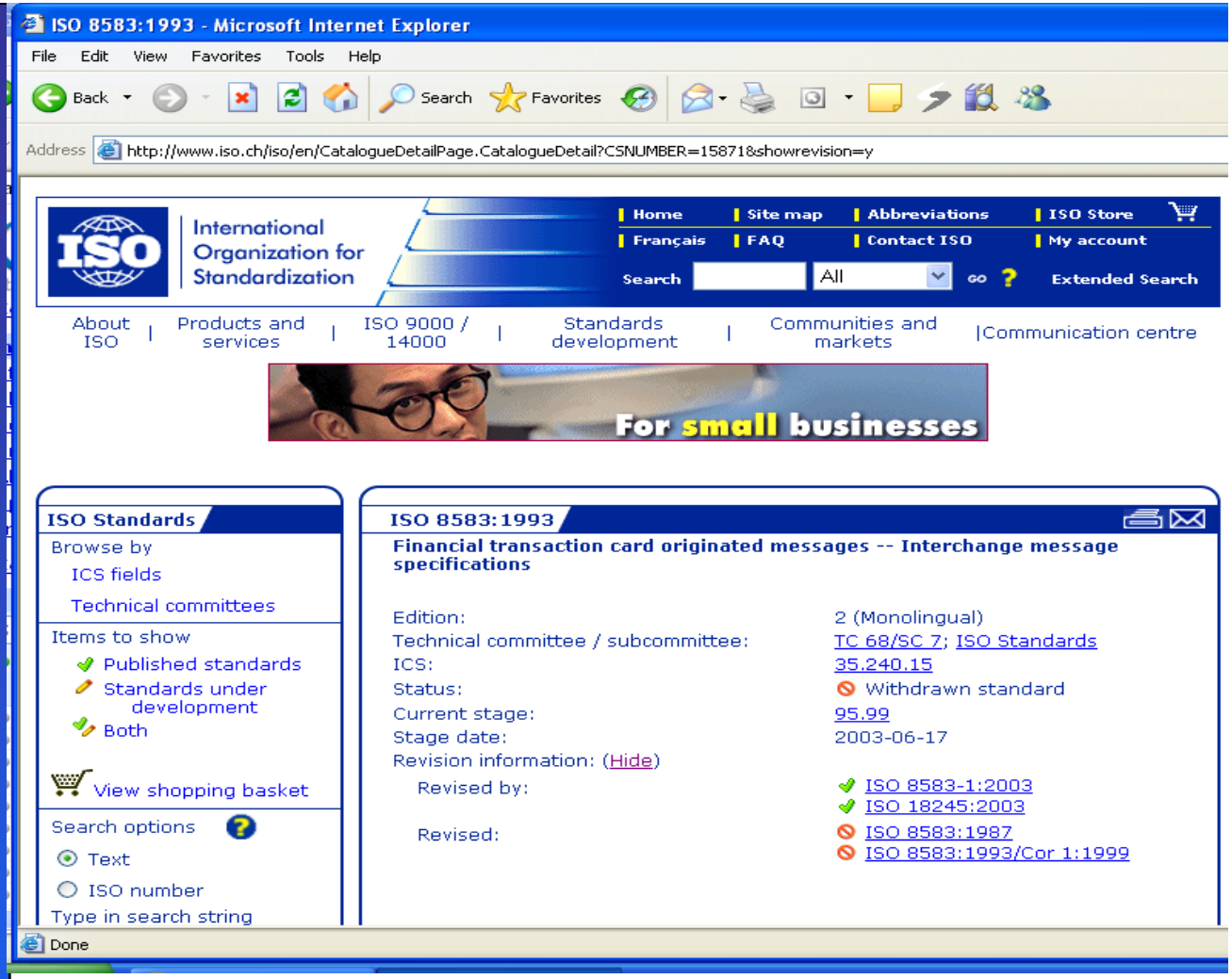
SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

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)

DELTA BANK

Issuer



ISO 8583 MESSAGES

Message concepts

- Sender
- Receiver

- Request
  - Where the sender informs the receiver that **a transaction is in process**.
- Instruction
  - Where the sender notifies the receiver of an **activity to be taken**.
- Advice
  - Message where the sender notifies the receiver **of an activity that has been taken**, **requiring no approval but requiring a response**. *(Confirm)*
- Notification
  - Where the sender notifies the receiver of **an activity taken.** *(Affirm)*
- Repeat
  - Resending a message for which no response was received within expected time.
- Response/Acknowledgement

Message format

- **An ISO 8583 message is made of the following parts:**
  - Message Type Indicator (MTI)
  - One or two message bitmaps, indicating which data elements are present .
  - A series of data elements, the fields of the message
- **Let's understand the "ABCD" of MTI**
  - **"A"** is version number –
    - **Example: "0" is 1987, "1" is 1993 and "2" is 2003**
  - **"B"** is message class –
    - **Example: "1" is Authorisation, "2" is Financial Presentment**
  - "**C**" is message function
    - **Example : "0" is Request, "1" is Request Response,**
  - **"D"** is transaction originator *(Note : Not the message originator)*
    - **Example: "0" is Acquirer, "2" is Card Issuer**

MVLCO

A	B	C	D
Version of ISO8583	Message Class	Function of the message	Who initiated the transaction
0xxx – ISO 8583:1987	x1xx – Authorisation Message	xx0x – Request	xxx0 – Acquirer
1xxx – ISO 8583:1993	x2xx – Financial Message	xx1x – Request Response	xxx1 – Acquirer Repeat
2xxx – ISO 8583:2003	x3xx – File Action Message	xx2x – Advice	xxx2 – Issuer
	x4xx – Reversal Message	xx3x – Advice Response	xxx3 – Issuer Repeat
	x5xx – Reconciliation Message	xx4x – Notification	xxx4 – Other
	x6xx – Administrative Message	xx8x – Response Ack.	xxx5 – Other Repeat
	x7xx – Fee Collection Message	xx8x – Negative Ack.	
	x8xx – Network Management		

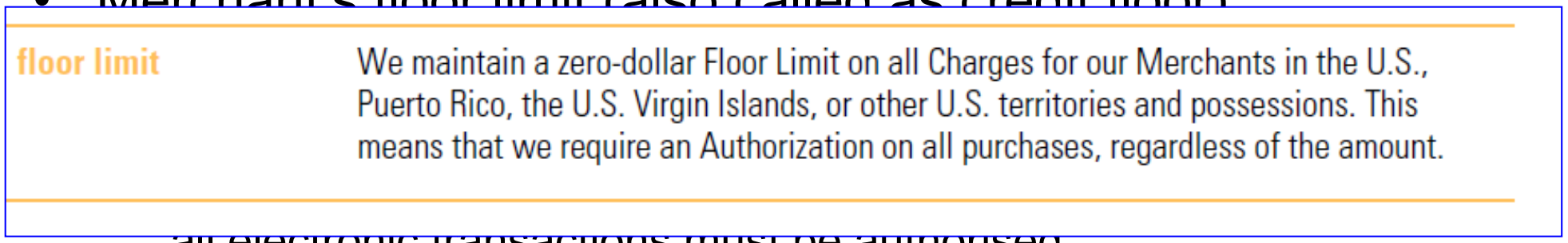
CFO

Message class	Originator	Request	Request repeat	Request response	Advice	Advice repeat	Advice response	Notification	Notification acknow-ledgement	Instruction	Instruction acknow-ledgement
Authorization	Acquirer	100	101	110	120	121	130	140	150		
Verification	Other	104	105	114	124	125	134	144	154		
Financial presentment	Acquirer	200	201	210	220	221	230	240	250		
File action	Acquirer							340	350		
	Card issuer									362	372
	Other	304	305	314	324	325	334	344	354	364	374
Reversal	Acquirer				420	421	430	440	450		
Chargeback	Card issuer				422	423	432	442	452		
Reconciliation	Acquirer	500	501	510	520	521	530	540	550		
	Card issuer	502	503	512	522	523	532	542	552		
Administration	Acquirer							640	650		
	Card issuer	602	603	612						662	672
	Other	604	605	614	624	625	634	644	654		
Fee collection	Acquirer				720	721	730	740	750		
	Card issuer				722	723	732	742	752		
Network management	Other	804	805	814	824	825	834	844	854		

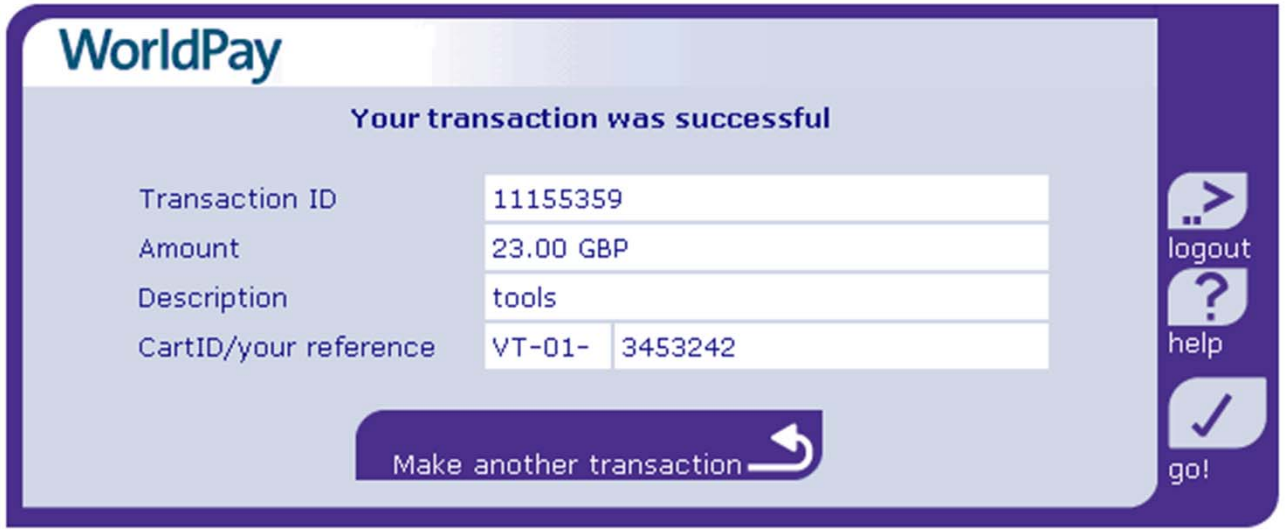
EMV AND NON-EMV ONLINE TRANSACTION PROCESSING

Concepts

- Manual processing
  - Embossed card
  - Checking the card recovery bulletin
- Electronic processing
  - Magstripe swipe/Chip Insert/Contactless and NFC waive
  - Hand key (Manual Entry) Processing
- Customer's credit limit
  - Over-limit transactions
- Merchant's floor limit (also called as credit floor)



all electronic transactions must be authorised.



MVLCO

AAA

AUTHENTICATION, ACCOUNTING, AUTHORISATION - AAA

CUSTOMER AUTHENTICATION

Authentication

I ♥ PIN

MVLCO

- **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

Chip and PIN

VERIFIED by VISA

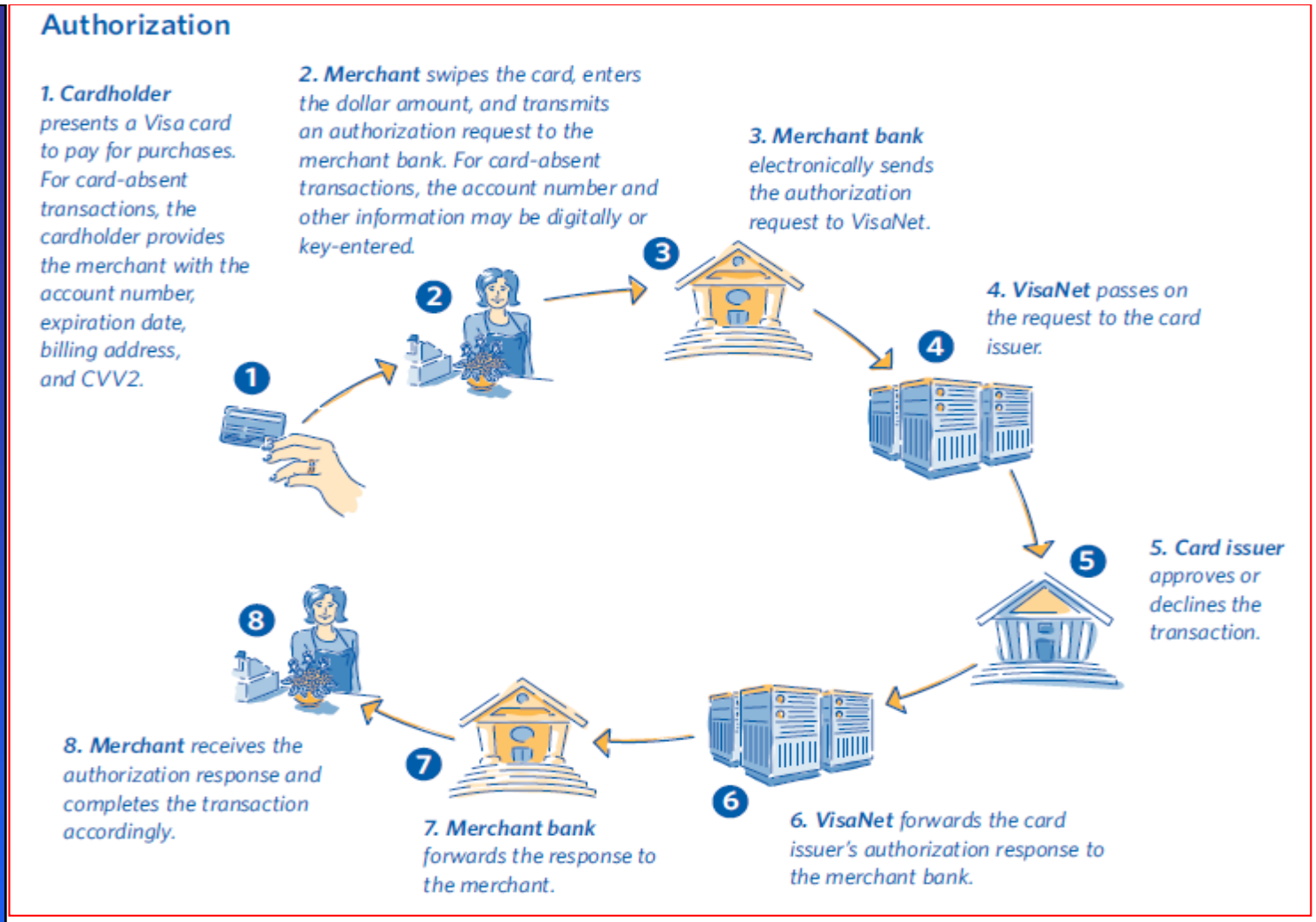
MasterCard SecureCode for Online Merchants

Building Consumer Confidence, Extending Your Market Reach

Dynamic passcode reader

RuPay®

Rupay Paysecure

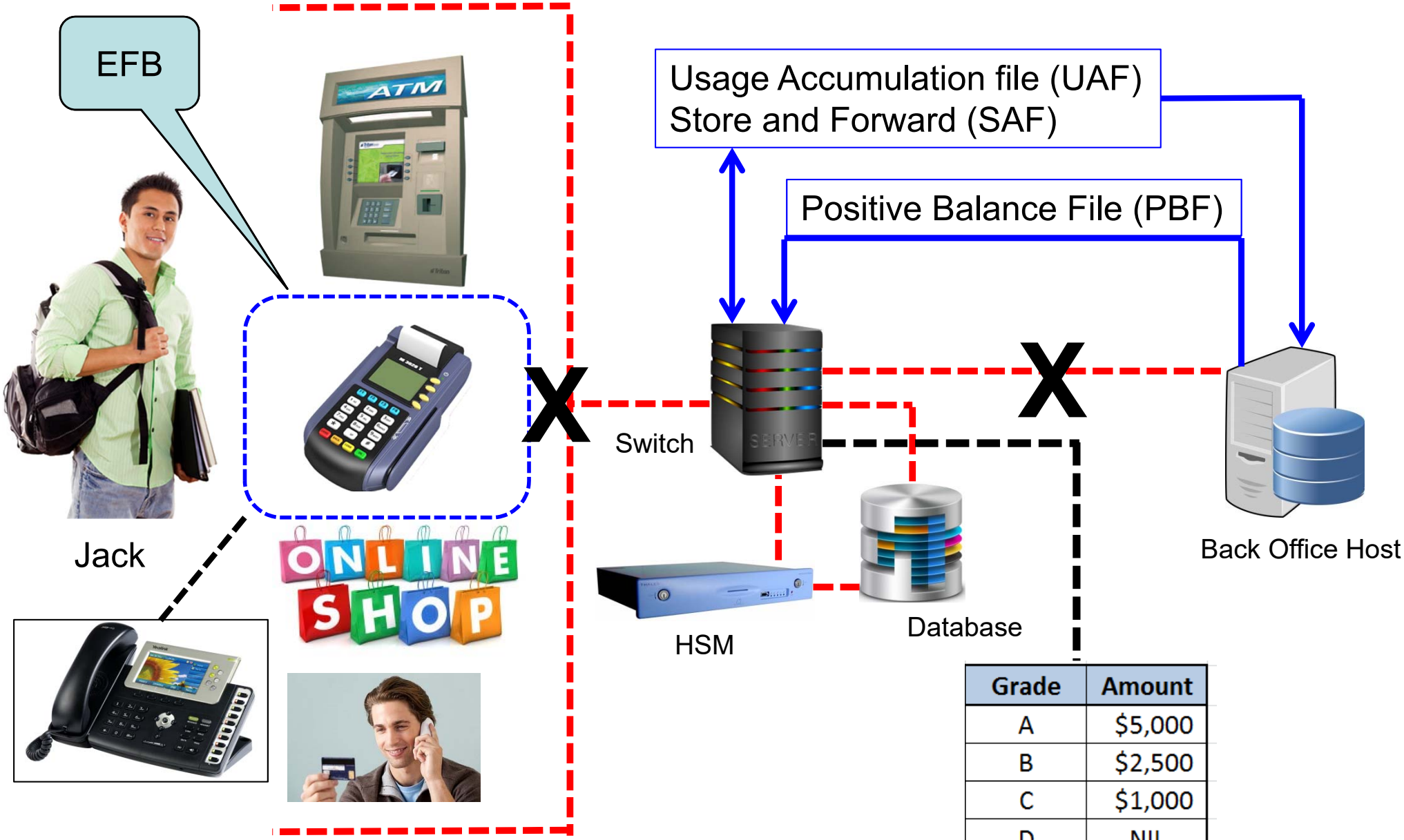


ACCOUNTING AND AUTHORISATION

Electronic authorisation

- **Batch mode v/s. real time authorisation**
- **Online authorisation**
  - Positive/Negative/Negative with 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**
  - STIP 1 and STIP 2

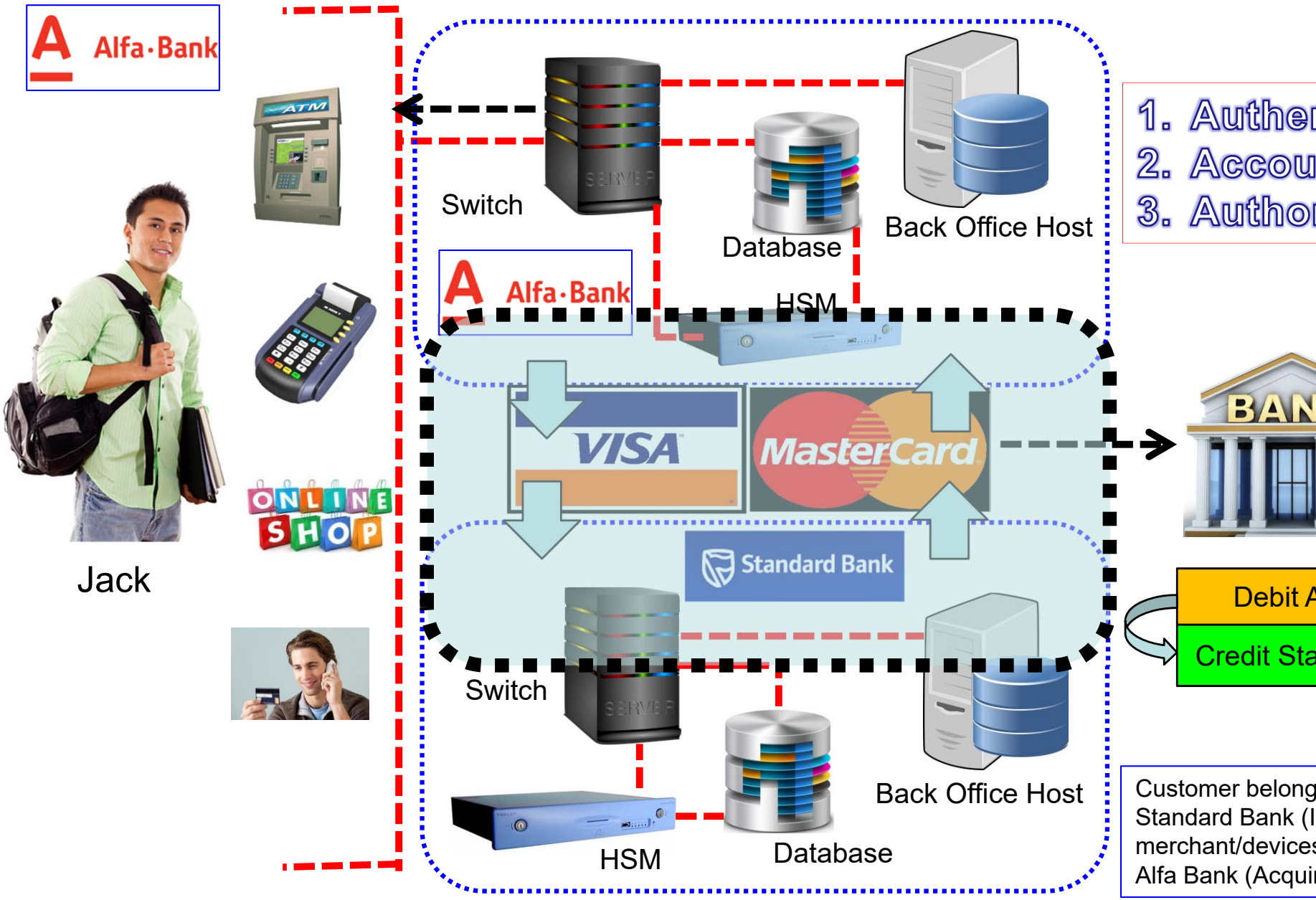
Recall ! On us transaction



Grade	Amount
A	$5,000
B	$2,500
C	$1,000
D	NIL

Recall! Off us transaction

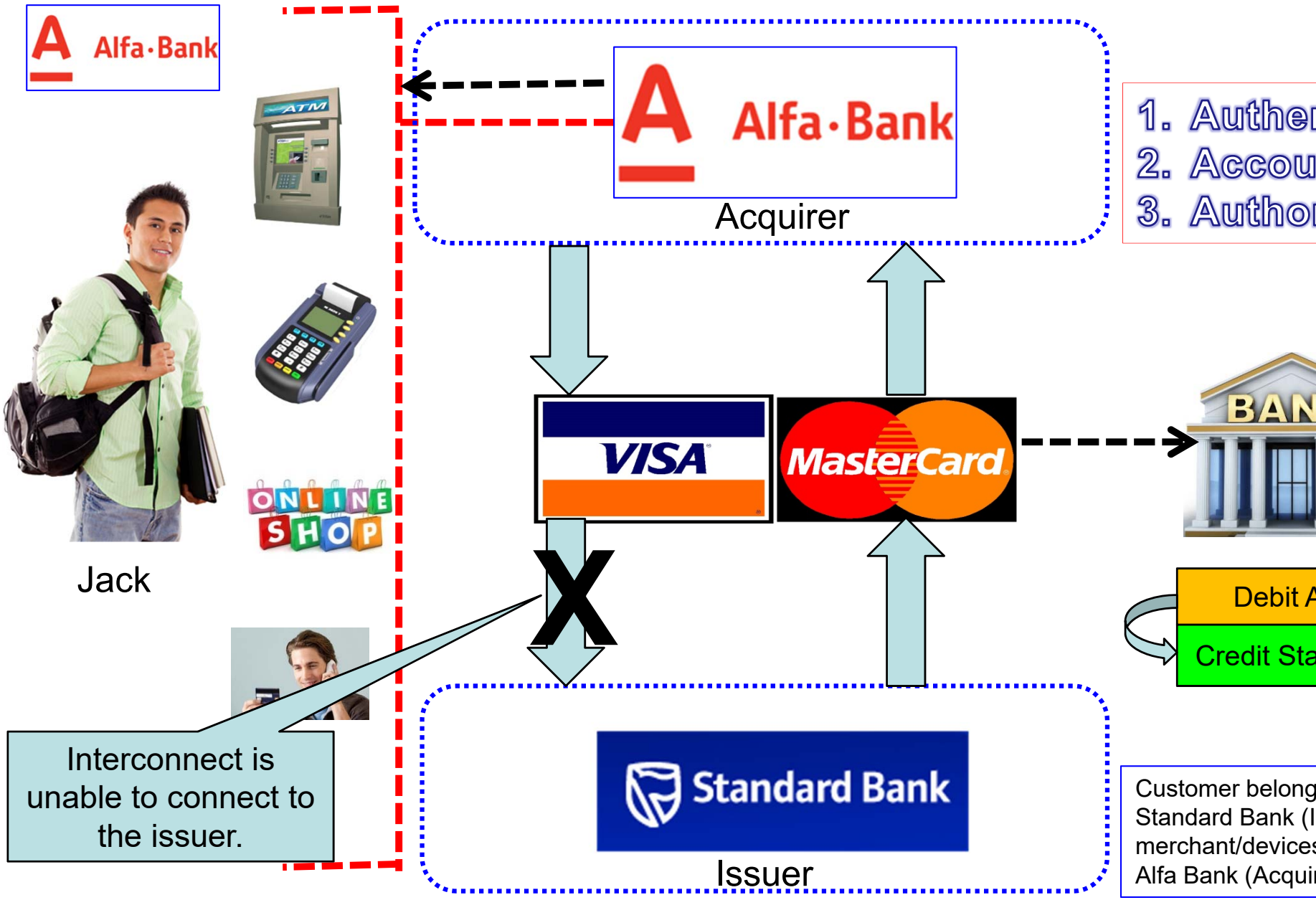
MVLCO



1. Authenticate
2. Account
3. Authorise

Customer belongs to Standard Bank (Issuer) and merchant/devices belong to Alfa Bank (Acquirer).

Recall! Off us transaction

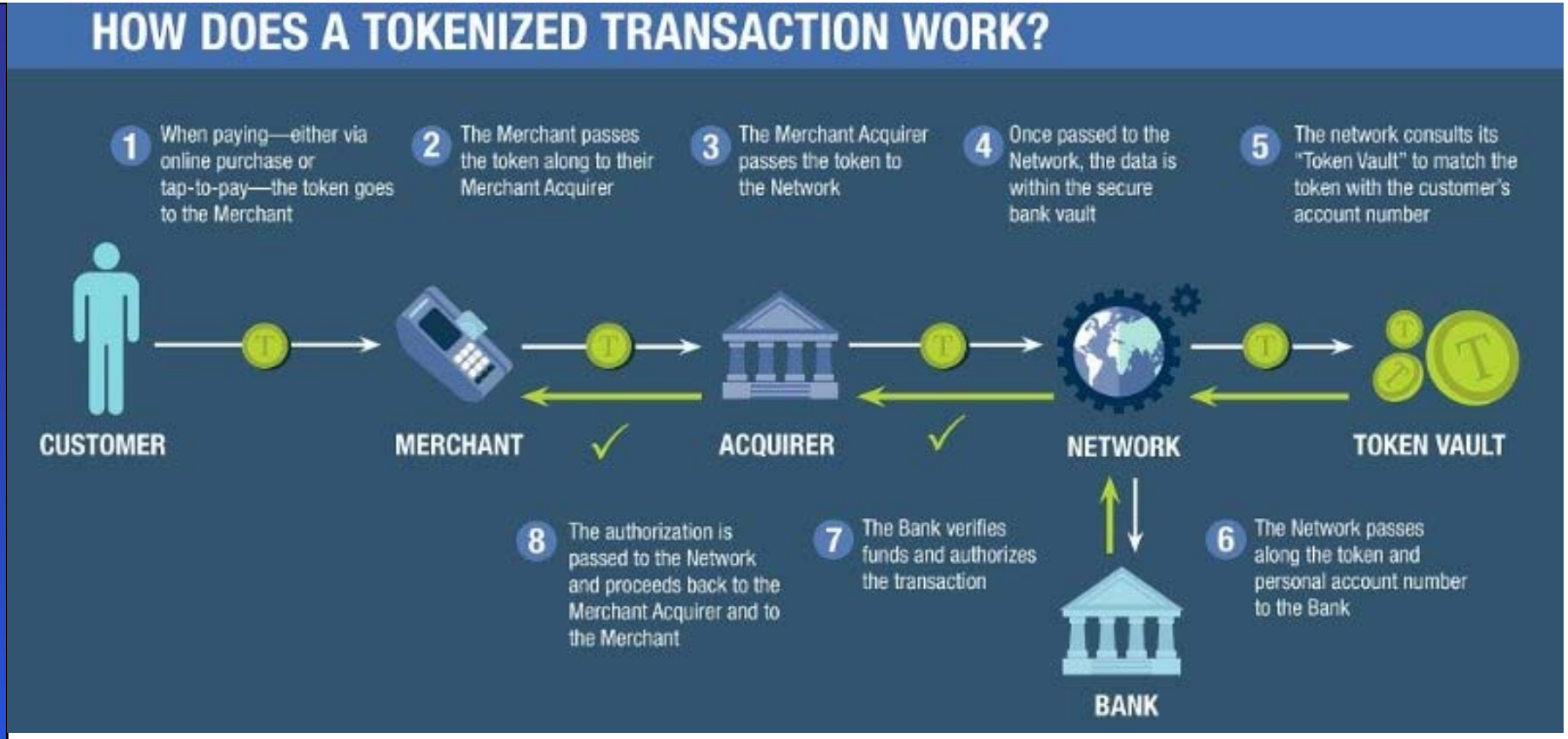


Interconnect authorisation processes including STIP process (1)

- **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.



MVLCO

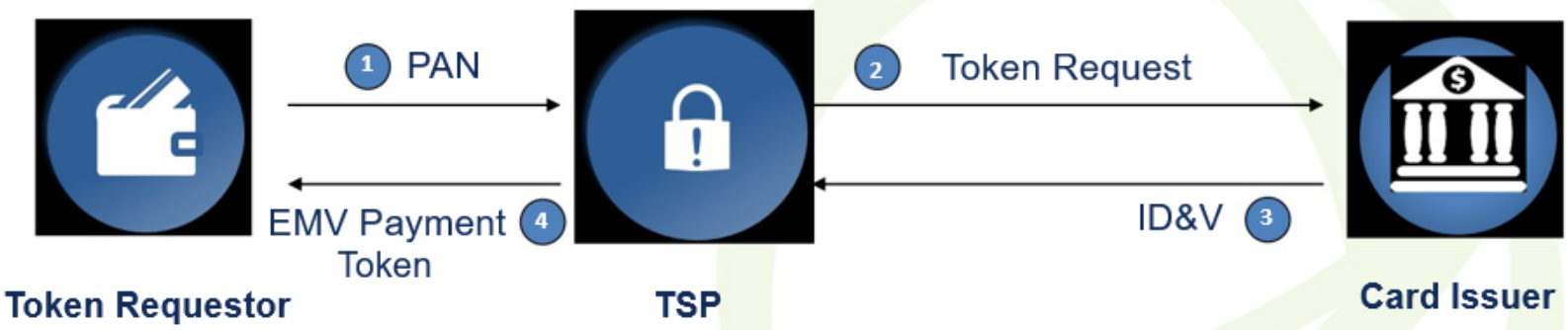
TOKENISATION

Token issue process

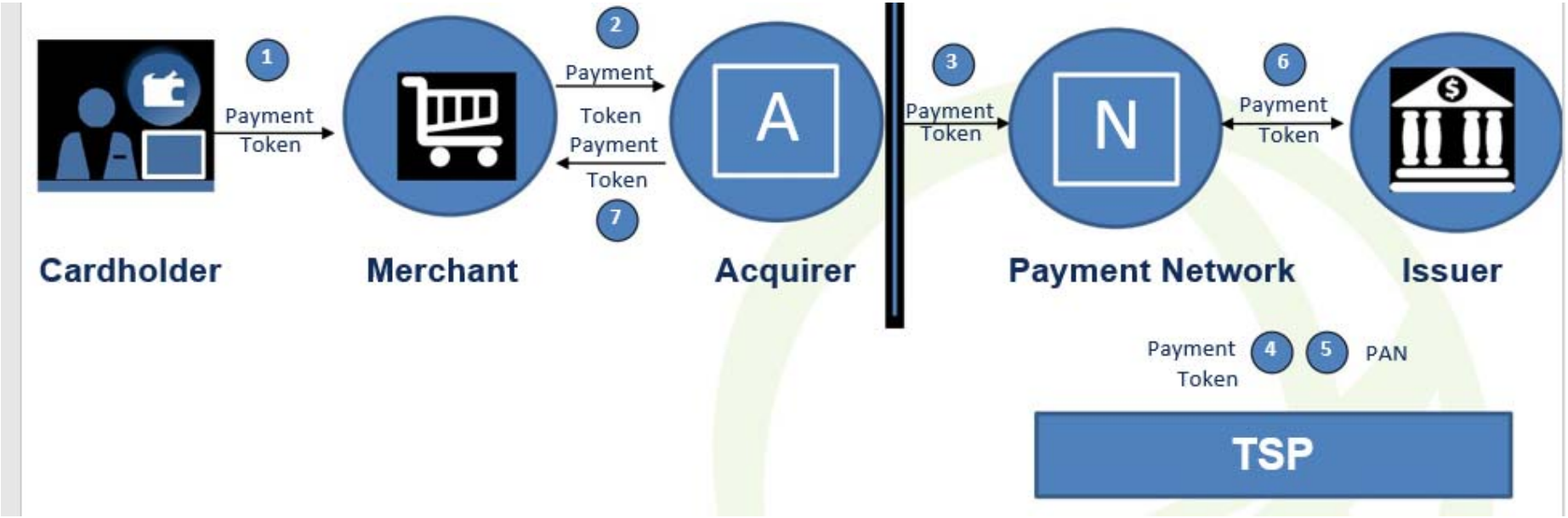
EMV Payment Token requests are made to a TSP. The token requestor, TSP and card issuer can all participate in ID&V. A token requestor can be a wallet, merchant, etc.

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

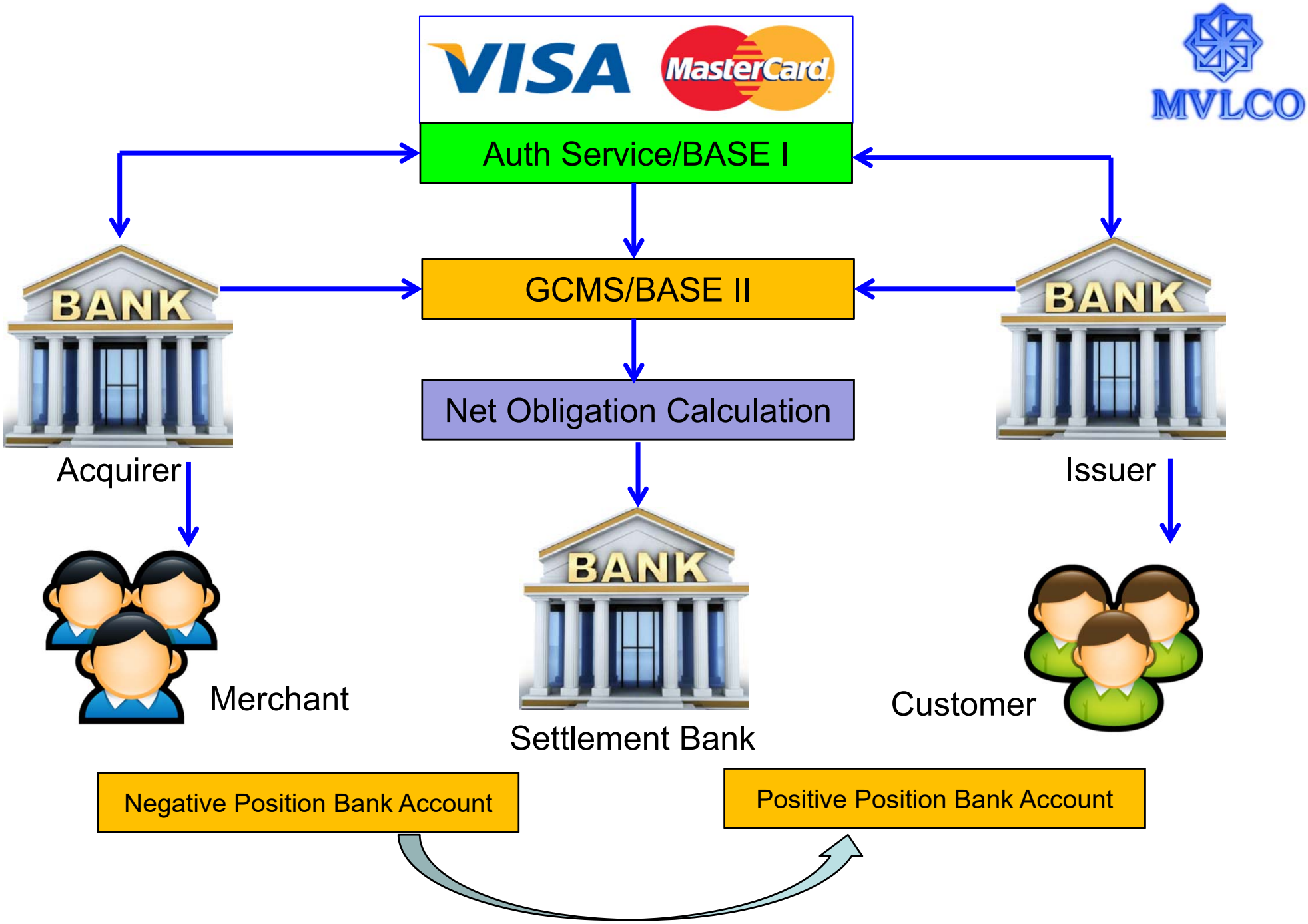
(4) and (5) Payment token is de-tokenised into a PAN by the TSP; card issuer makes authorization decision and returns PAN to TSP

(6) and (7) TSP re-tokenises the PAN and the authorisation response flows back through the acquirer to the merchant

INTERBANK SETTLEMENT

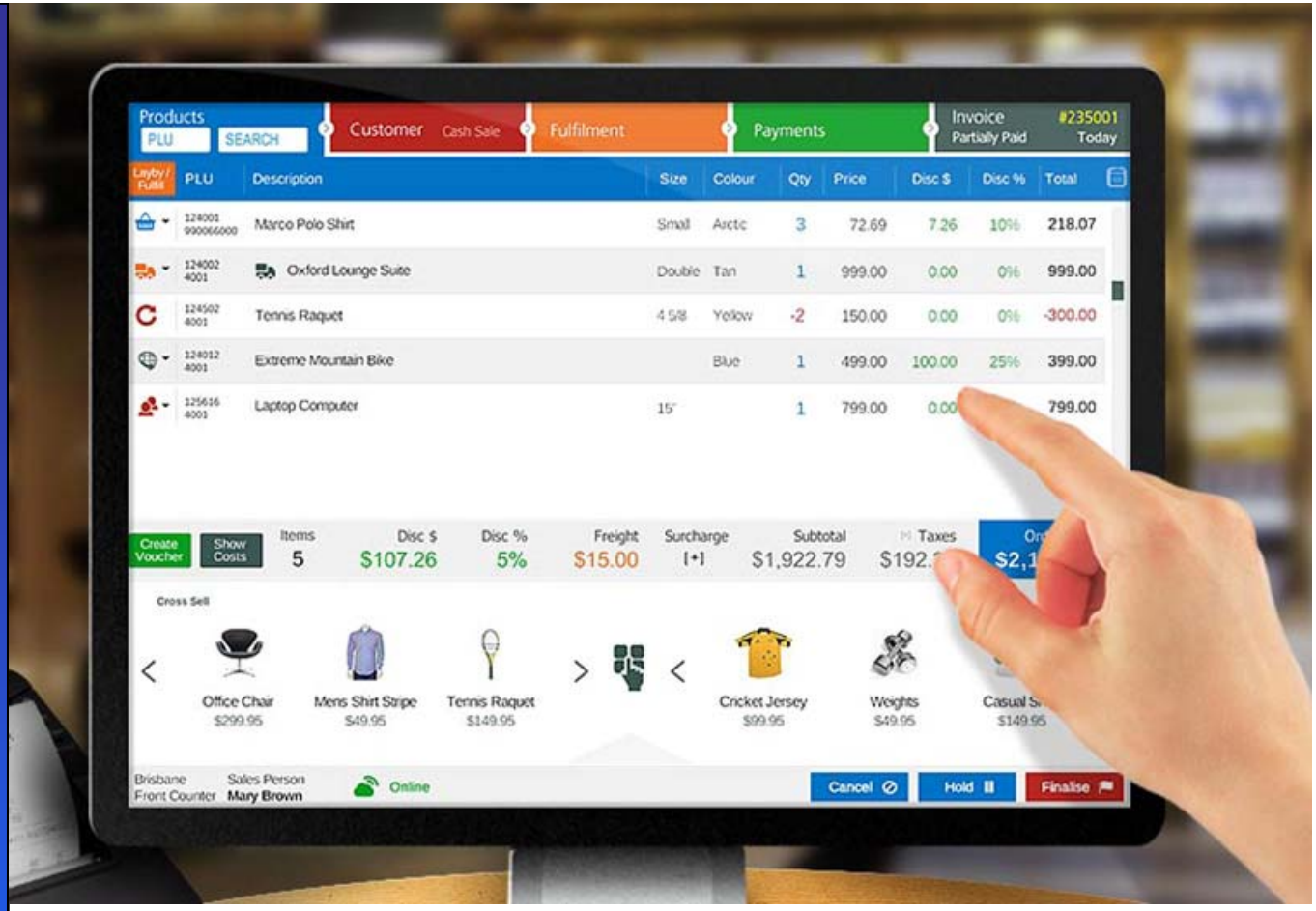
Interbank settlement

- 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
MasterCard
Auth Service/BASE I
GCMS/BASE II
Net Obligation Calculation
BANK
Acquirer
BANK
Issuer
BANK
Settlement Bank
Merchant
Customer
Negative Position Bank Account
Positive Position Bank Account

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.



MERCHANT TRANSACTIONS AND PRESENTMENT

Merchant transactions

- Sale
  - Tab processing
- Void/reversal – before settlement
- Refund processing – no cash refund
- Cash out
- MOTO transaction
- Preauthorisation hold
- Tip/gratuity processing
- Split tender processing
- Deposit and balance amount authorisation
- Convenience fee

Visa Tendered £6.90

Card : VISA CREDIT
Number : ************4496
PAN Seq : 00
App ID : A0000000031010
App Date : 01/03/08 - 31/01/13
Cryptogram : 40/B6C3555EA87911C7
Merchant ID: 70728382
Terminal ID: 23107748
TVR : 0080008000
TSI : F800
Captured : CHIP
Cust. Ver. : 410302
Auth. Code : 907748

TRANSACTION CURRENCY
Euro €8.20
Exchange Rate: EUR1.1882/£

CardHolder has chosen to pay in Euro. This transaction is based on REUTERS WHOLESALE INTERBANK exchange rate plus 2.95% international conversion margin. This is not an additional fee and replaces currency conversion charges normally applied. My choice is final. Transactions may also be conducted in Sterling.

Currency conversion service is provided by Harrods Limited.

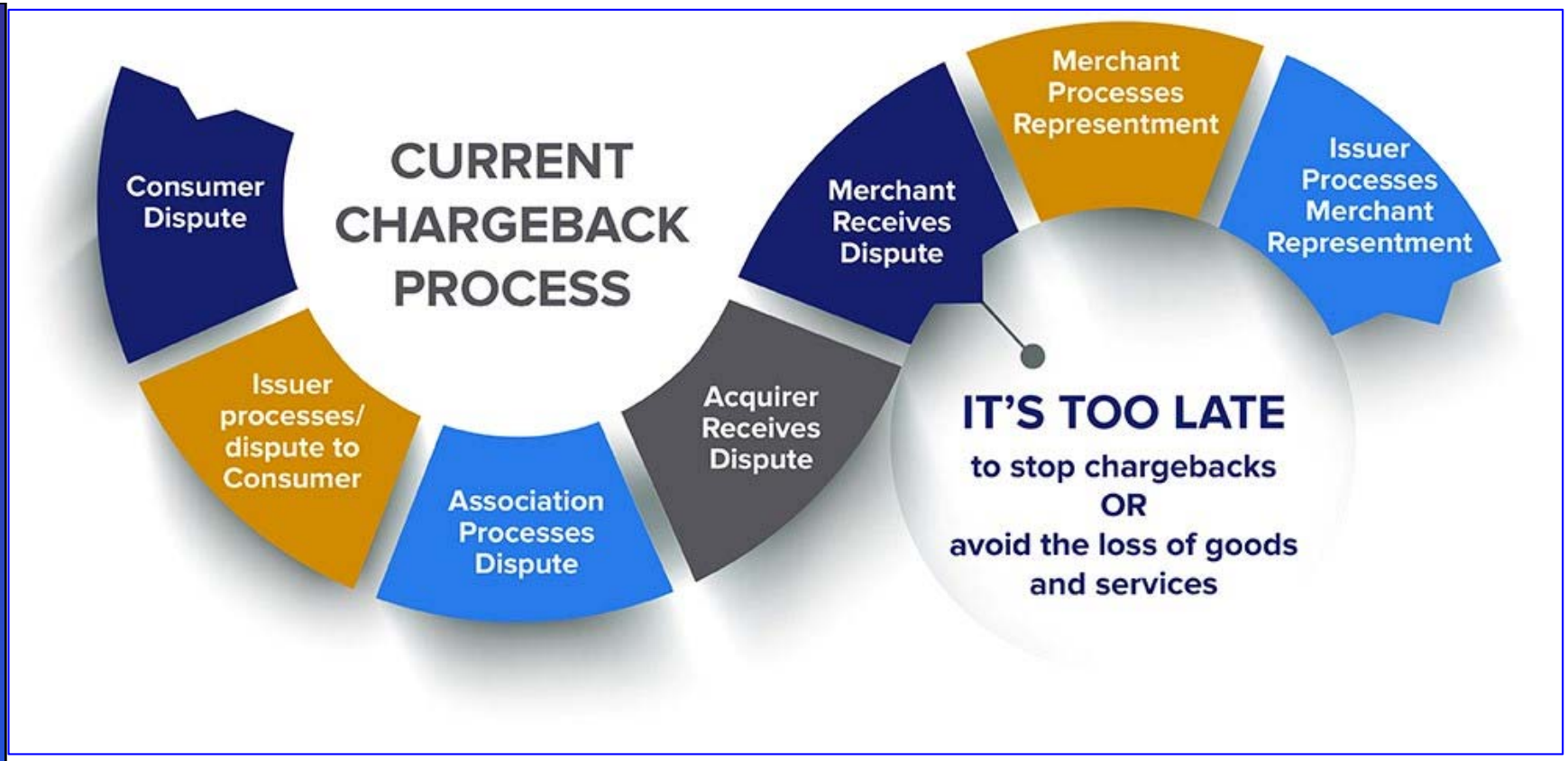
MVLCO

About Customer Preferred Currency

DYNAMIC CURRENCY CONVERSION

What is DCC or CPC ?

- This feature provides international credit card customers the option of converting foreign currency purchases/cash transactions into their card's billing currency at the time of transaction.
- If the terminal is enabled for Dynamic Currency Conversion (DCC), it is possible to process transactions in the cardholder's home currency.
- DCC is optional.
- This is only offered on credit transactions on MasterCard and Visa for the certain currencies e.g. United States Dollar (USD), Canadian Dollar (CAD), Euros (EUR), Pounds Sterling (GBP), Japanese Yen (JPY), Singapore Dollars (SGD), Hong Kong Dollars (HKD), and New Zealand Dollars (NZD).
- The exchange rates in the terminal will update automatically at the time of the DCC.
- DCC is prohibited in some countries for ATM and cash out transactions.



MVLCO

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 representment 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 chargebackrates.

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

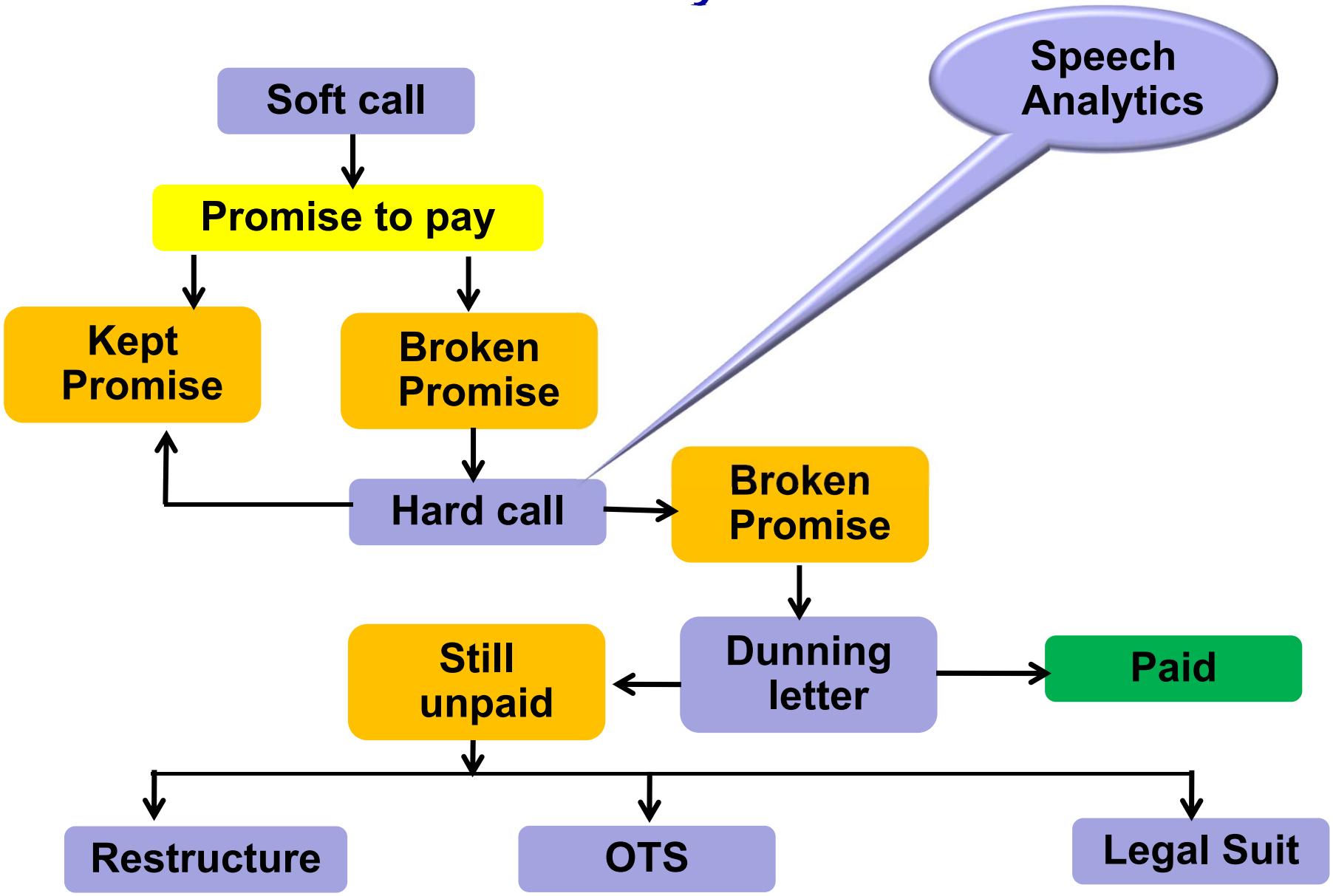
ID#: 081010-010410-0002445

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

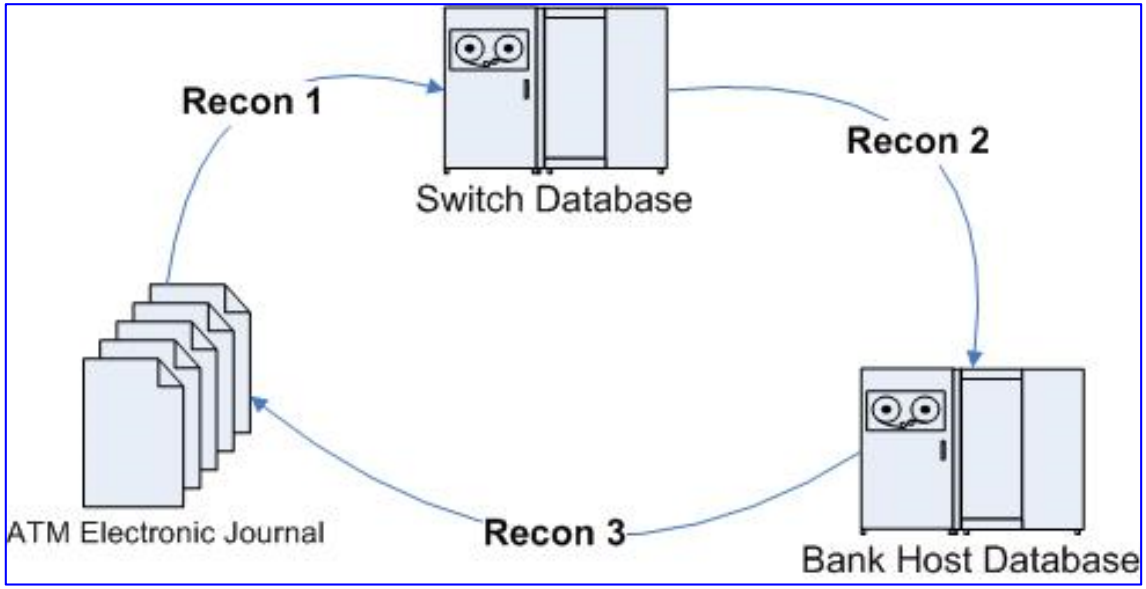


MVLCO

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
Application fraud	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
Lost and stolen credit cards	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
Non-receipt (mail intercept) fraud	Individual's mail is intercepted by criminal		Card activation process
Counterfeit cards	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
Account takeover	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
Bust-out-fraud	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 legitimate users	Closure of account if sudden deviation from model behavior

DATA BREACH AND HACKING

Card frauds and security lapses

- February 18, 2005 – Bank of America claimed that it had lost more than 1.2 million customer records – though it said there was no evidence that the data had fallen into the hands of criminals.
- June 16, 2005 – CardSystems, a merchant payment-processing provider, was sued in a series of class action cases alleging that it failed to adequately protect the personal information of 40 million customers. CardSystems' business faced collapse as VISA and American Express cut their ties with the company, prohibiting it from processing their card data. CardSystems was subsequently acquired by another company.
- January 17, 2007 – TJX Companies Inc. publicly disclosed that they had experienced an unauthorized intrusion into the electronic credit/debit card processing system. In what is considered the most glamorous security breaches to date, as much as 45,700,000 credit/debit card account numbers and over 455,000 merchandise return records (containing customer names and driver's license numbers) were stolen from the company's IT system.

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.

MVLCO

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

MVLCO

Thank You !